



Universidad  
Carlos III de Madrid

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA INFORMÁTICA

PROYECTO FIN DE CARRERA

# **Emulación de Tarjetas NFC en Android**

Autor: Francisco Fernández Díaz

Tutor: Pedro Peris López

Cotutor: Pablo Picazo Sánchez

Leganés, Mayo de 2015



Título: Emulación de Tarjetas NFC en Android

Autor: Francisco Fernández Díaz

Tutor: Pedro Peris López

Cotutor: Pablo Picazo Sánchez

## EL TRIBUNAL

Presidente: \_\_\_\_\_

Vocal: \_\_\_\_\_

Secretario: \_\_\_\_\_

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día \_\_ de \_\_\_\_\_ de 20\_\_ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO

PRESIDENTE



## AGRADECIMIENTOS

*Dedicar el final de esta etapa de mi vida a mi familia, siempre han estado a mi lado animándome, permitiendo que me creara un futuro a mi gusto del que no me arrepintiera y ayudándome a conseguirlo. A mis padres, Alfonso y Francisca, por haberme proporcionado todo lo necesario para que pudiera realizar unos estudios de estas magnitudes y sin presionarme para que así disfrutara y aprendiera todo lo posible de ello, a mi hermana Noelia que siempre sabe cómo hacerme reír en los momentos complicados, y a mis abuelos que desde el primer momento nunca duraron en que podía conseguirlo y siempre se han sentido orgullosos.*

*Dedicar también todo este trabajo a mis amigos, Rafael, Israel y Pepe, que llevamos muchos años de amistad y nunca me han abandonado a pesar del poco tiempo pasado con ellos durante el tiempo que ha durado esta carrera. A los compañeros de la universidad, Coral, Adrián, Roberto, Laura, Luis, Verónica, Daniel, Christian y Jose, por aguantarme y haber pasado tan buenos momentos juntos, riéndonos por lo bueno y lo malo y pasándolo bien tanto en el ámbito de los estudios como fuera de él.*

*También se lo agradezco a mis tutores de este proyecto, por la paciencia que han tenido durante el periodo de su desarrollo y toda la ayuda que me han ofrecido, así como al resto de profesores que a lo largo de la carrera me han hecho crecer personal y profesionalmente.*

*Por último quiero dedicar este proyecto de fin de carrera a Ángel, mi abuelo materno, el cual falleció durante el desarrollo de las etapas finales de este proyecto.*

**!!!Muchas gracias a todos!!!**



---

## RESUMEN

Hoy en día las personas cada vez tienen la necesidad de llevar consigo muchas tarjetas, ya sean de crédito, para acceder al trabajo, hoteles o al transporte, y eso puede ocasionar problemas, ya sea por olvidar alguna entre tantas, robo, pérdida o simplemente que el usuario no quiera llevar todas consigo.

Además los smartphones/teléfonos móviles son utilizados para ver noticias, llamar a otras personas, jugar, etc. Son pequeños ordenadores que llevamos en el bolsillo y que forman parte de nuestra vida diaria.

Entonces, ¿cómo podríamos utilizarlos en lugar de las tarjetas físicas? La solución es la tecnología Near Field Communication (NFC). Esta permite interactuar con las tarjetas y así un usuario podría usarlo para realizar pagos, accesos de control y acceso a transportes, es decir, lo mismo que si llevara la tarjeta física con él.

El propósito de este proyecto es desarrollar una aplicación Android para almacenar, administrar y transmitir tarjetas RFID desde el smartphone o teléfono móvil en lugar de llevar todas las tarjetas originales en el bolsillo del propietario. Asimismo, todas las claves usadas deben ser almacenadas en un servidor de la nube, Google App Engine, para obtener datos estadísticos de las más usadas para posteriormente hacer una investigación sobre ello.

## ABSTRACT

Nowadays people the need to carry a lot of physical cards, either credit, to grant access to the office, hotels, public transport... This can cause a lot of issues, either by forgetting one among many, theft, loss or just the user does not want to carry them all.

Besides, the smartphones / mobile phones are used to watch news, call other people, play, etc. They are also small computers that we carry in our pocket and are part of our daily life.

So, how could we use them instead of physical cards? The solution is the Near Field Communication (NFC) technology. This technology can interact with cards so user could make payments with it, access control and access to transport, with the same behavior as if user had the physical card with him.

The purpose of this project is to develop an Android application to store, manage and transmit RFID cards from the smartphone or mobile phone instead of taking all the original cards in the owner's pocket. Furthermore, all the keys used must be stored on a server in the cloud, Google App Engine, to obtain statistical data of the most used so there can be do some research on it afterwards.



## Índice de contenido

AGRADECIMIENTOS.....	v
RESUMEN .....	vii
ABSTRACT .....	viii
Índice de contenido.....	ix
Índice de figuras .....	xiv
Índice de tablas.....	xviii
CAPÍTULO 1: INTRODUCCIÓN Y OBJETIVOS.....	1
1.    Introducción.....	2
2.    Objetivos .....	4
3.    Fases del desarrollo.....	5
4.    Motivación.....	6
5.    Estructura del documento .....	6
CAPÍTULO 2: ESTADO DEL ARTE.....	8
1.    NFC.....	9
1.1.    Introducción.....	9
1.1.1.    ¿Qué aplicaciones tiene? .....	10
1.2.    Características NFC.....	10
1.3.    Estandarización.....	11
1.3.1.    Arquitectura NFC.....	13
1.4.    Etiquetas NFC .....	16
1.4.1.    Mifare .....	17
1.4.1.1.    Tipos etiquetas Mifare .....	17
1.5.    Lectores NFC .....	21
1.5.1.    Conectividad .....	22
1.5.2.    Compatible con modo lectura/escritura .....	22
1.5.3.    Compatible con modo emulación de tarjeta.....	22

---

1.6.	Flujo de comunicación Mifare Classic.....	22
1.6.1.	Solicitud estándar/Solicitud todos.....	24
1.6.2.	Bucle anticolisión.....	24
1.6.3.	Seleccionar tarjeta.....	24
1.6.4.	Autenticación a tres fases.....	25
1.6.5.	Halt.....	25
1.7.	Crypto1.....	26
1.7.1.	Cifrado de flujo.....	26
1.7.1.1.	Generador de clave.....	26
1.7.2.	Generador de números pseudoaleatorios.....	27
1.7.3.	Flujo interno del algoritmo Crypto1.....	28
1.7.3.1.	Inicialización.....	28
1.7.3.2.	Encriptación.....	28
1.8.	Herramientas de ataque NFC.....	29
1.8.1.	Proxmark3.....	29
1.8.2.	LibNFC.....	30
1.8.3.	Crapto1.....	30
2.	Android.....	31
2.1.	Introducción.....	31
2.1.1.	¿Qué es Android?.....	31
2.2.	Arquitectura.....	32
2.3.	NFC en Android.....	34
3.	SQLite.....	34
4.	Android CyanogenMod.....	35
5.	Google App Engine.....	36
CAPÍTULO 3: DESARROLLO TÉCNICO DEL PFC.....		37
1.	Análisis.....	38
1.1.	Requisitos de usuario.....	38

---

1.1.1.	Requisitos de capacidad .....	39
1.1.2.	Requisitos de restricción .....	41
1.1.	Casos de uso .....	48
1.1.1.	Diagrama de casos de uso .....	49
1.1.2.	Especificación detallada de los casos de uso .....	50
1.2.	Requisitos software .....	60
1.2.1.	Requisitos funcionales .....	62
1.2.2.	Requisitos no funcionales .....	73
1.2.2.1.	Requisitos software no funcionales de operación.....	73
1.2.2.2.	Requisitos software no funcionales de interfaz.....	81
1.2.2.3.	Requisitos software no funcionales de recursos.....	90
1.2.2.4.	Requisitos software no funcionales de rendimiento.....	91
1.3.	Matrices de trazabilidad .....	93
1.3.1.	Matriz de trazabilidad entre requisitos de usuario y requisitos software funcionales .....	93
1.3.2.	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de operación.....	95
1.3.3.	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de interfaz.....	97
1.3.4.	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de recursos .....	98
1.3.5.	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de rendimiento .....	98
2.	Diseño.....	99
2.1.	Arquitectura .....	99
2.1.1.	Alternativas de diseño .....	99
2.1.2.	Diagrama de componentes .....	100
2.2.	Diagrama de clases.....	102
2.3.	Diseño de base de datos.....	103

CAPÍTULO 4: PRUEBAS.....	105
1. Pruebas del sistema.....	106
1.1. Especificación de pruebas del sistema .....	107
1.2. Trazabilidad entre requisitos software funcionales y pruebas del sistema .....	122
2. Resultados .....	124
2.1. Prueba 1 – Lectura tarjeta Mifare Ultralight.....	124
2.2. Prueba 2 – Lectura tarjeta Mifare Classic 1K .....	125
2.3. Prueba 3 – Lectura tarjeta Mifare Classic 1K .....	126
2.4. Prueba 4 – Lectura tarjeta Mifare Classic 4K (tarjeta de transporte).....	126
2.5. Prueba 5 – Escritura en tarjeta Mifare Classic 1K.....	130
CAPÍTULO 5: CONCLUSIONES Y FUTURAS LÍNEAS DE TRABAJO .....	133
1. Conclusiones .....	134
2. Futuras líneas de trabajo.....	136
REFERENCIAS .....	137
ANEXOS .....	142
ANEXO I: Acrónimos y Definiciones.....	143
1. Acrónimos .....	144
2. Definiciones .....	145
ANEXO II: Gestión del Proyecto .....	149
1. Planificación del Proyecto .....	150
2. Presupuesto del Proyecto .....	152
2.1. Coste del personal.....	152
2.2. Coste de equipos .....	152
2.3. Coste de software .....	153
2.4. Material fungible.....	153
2.5. Costes directos totales .....	153
2.6. Costes indirectos.....	154
2.7. Beneficio .....	154

---

2.8.	Margen de riesgo.....	154
2.9.	Presupuesto total .....	154
ANEXO III:	Manual de Usuario.....	155
1.	Acceso Inicial .....	156
2.	Pantalla Principal .....	156
3.	Leer .....	157
3.1.	Ver como transporte .....	162
3.2.	Ver como ASCII.....	164
3.3.	Ver condiciones de acceso .....	166
4.	Escribir.....	167
5.	Ver tarjetas escaneadas.....	170
5.1.	Crear tarjeta.....	171
5.2.	Editar tarjeta.....	173
5.3.	Borrar tarjeta .....	173
5.4.	Importar tarjetas .....	174
6.	Claves.....	175
6.1.	Crear clave .....	177
6.2.	Editar clave .....	178
6.3.	Borrar clave .....	178
6.4.	Importar claves.....	179
6.5.	Grupos de claves .....	180
2.3.1.	Crear grupo de claves .....	180
2.3.2.	Editar grupo de claves .....	182
2.3.3.	Borrar grupo de claves .....	184
7.	Ver estadísticas de uso .....	184
8.	Activar tecnología NFC.....	186
ANEXO IV:	Scripts y Modificaciones de Aplicaciones .....	187

## Índice de figuras

Ilustración 1: NFC vs. otras tecnologías [33].....	3
Ilustración 2: Aplicaciones NFC.....	10
Ilustración 3: Estructura protocolo NFC [39] .....	12
Ilustración 4: Arquitectura NFC.....	13
Ilustración 5: Estructura mensaje NDEF [38] .....	14
Ilustración 6: Formato registro NDEF [38] .....	15
Ilustración 7: Estructura memoria Mifare Classic 4K .....	18
Ilustración 8: Estructura memoria Mifare Ultralight .....	20
Ilustración 9: Comandos Mifare Classic .....	23
Ilustración 10: Flujo de comunicación Mifare Classic.....	23
Ilustración 11: Crypto1 – Estructura cifrado de flujo.....	26
Ilustración 12: Crypto1 – Estructura del generador de números pseudoaleatorios .....	27
Ilustración 13: Crypto1 – Estructura completa .....	29
Ilustración 14: Versiones de Android .....	32
Ilustración 15: Casos de uso .....	49
Ilustración 16: Diagrama de componentes.....	100
Ilustración 17: Diagrama de clases.....	103
Ilustración 18: Modelo de datos del sistema .....	104
Ilustración 19: Prueba 1 – Resultado de dispositivo móvil (arriba) y del lector con LibNFC (abajo).....	124
Ilustración 20: Prueba 2 – Claves obtenidas a través de la Proxmark3 (arriba), resultado de dispositivo móvil (izquierda) y del lector con Mfoc (derecha) .....	125
Ilustración 21: Prueba 3 – Resultado de dispositivo móvil (izquierda) y del lector con Mfoc (derecha) .....	126
Ilustración 22: Prueba 4 – Resultado lectura de dispositivo móvil (izquierda) y del lector con Mfoc (derecha) .....	127

---

Ilustración 23: Prueba 4 – Decodificación información general de transporte con el dispositivo móvil.....	127
Ilustración 24: Prueba 4 – Decodificación información general de transporte con el lector y Mfoc GUI.....	128
Ilustración 25: Prueba 4 – Decodificación historial de viajes de transporte con el dispositivo móvil.....	128
Ilustración 26: Prueba 4 – Decodificación historial de viajes de transporte con el lector y Mfoc GUI .....	129
Ilustración 27: Prueba 4 – Decodificación subscripciones de transporte con el dispositivo móvil .....	129
Ilustración 28: Prueba 4 – Decodificación subscripciones de transporte con el lector y Mfoc GUI .....	130
Ilustración 29: Prueba 5 – Resultado modificación de tarjeta almacenada en el dispositivo móvil: hexadecimal (izquierda), ASCII (derecha) .....	131
Ilustración 30: Prueba 5 – Resultado lectura de dispositivo móvil de tarjeta modificada: hexadecimal (izquierda), ASCII (derecha).....	131
Ilustración 31: Prueba 5 – Resultado lectura con el lector y Mfoc de una tarjeta escrita.....	132
Ilustración 32: Diagrama de Gantt.....	151
Ilustración 33: Manual de usuario – Acceso inicial.....	156
Ilustración 34: Manual de usuario – Pantalla inicial.....	157
Ilustración 35: Manual de usuario – Acceder a leer .....	157
Ilustración 36: Manual de usuario – Selección de claves en lectura.....	158
Ilustración 37: Manual de usuario – Leer tarjeta.....	159
Ilustración 38: Manual de usuario – Limpiar lectura .....	159
Ilustración 39: Manual de usuario – Contenido tarjeta a guardar .....	160
Ilustración 40: Manual de usuario – Nuevo tipo de tarjeta.....	161
Ilustración 41: Manual de usuario – Guardar tarjeta .....	161
Ilustración 42: Manual de usuario – Tarjeta repetida .....	162
Ilustración 43: Manual de usuario – Ver como transporte – Opción menú.....	163

Ilustración 44: Manual de usuario – Ver como transporte - General .....	163
Ilustración 45: Manual de usuario – Ver como transporte - Historial.....	164
Ilustración 46: Manual de usuario – Ver como transporte - Subscripciones .....	164
Ilustración 47: Manual de usuario – Ver como ASCII – Opción menú .....	165
Ilustración 48: Manual de usuario – Ver como ASCII – Contenido en ASCII .....	165
Ilustración 49: Manual de usuario – Ver como ASCII – Contenido en ASCII .....	166
Ilustración 50: Manual de usuario – Ver condiciones de acceso – Opción menú.....	166
Ilustración 51: Manual de usuario – Ver condiciones de acceso .....	167
Ilustración 52: Manual de usuario – Acceder a escribir .....	167
Ilustración 53: Manual de usuario – Seleccionar tarjeta a escribir .....	168
Ilustración 54: Manual de usuario – Selección de claves en escritura.....	168
Ilustración 55: Manual de usuario – Confirmación escritura .....	169
Ilustración 56: Manual de usuario – Escribir todos los bloques posibles.....	170
Ilustración 57: Manual de usuario – Acceder a escaneados.....	170
Ilustración 58: Manual de usuario – Lista de tarjetas.....	171
Ilustración 59: Manual de usuario – Crear tarjeta .....	171
Ilustración 60: Manual de usuario – Seleccionar tipo de tarjeta a crear .....	172
Ilustración 61: Manual de usuario – Tarjeta Mifare Ultralight creada (izquierda); Tarjeta Mifare Classic Mini, 1K y 4K creada (derecha) .....	172
Ilustración 62: Manual de usuario – Editar tarjeta.....	173
Ilustración 63: Manual de usuario – Eliminar tarjeta.....	174
Ilustración 64: Manual de usuario – Importar tarjetas.....	174
Ilustración 65: Manual de usuario – Importar tarjetas – Configuración .....	175
Ilustración 66: Manual de usuario – Acceder a claves.....	176
Ilustración 67: Manual de usuario – Lista de claves (izquierda) y grupos de claves (derecha) .....	176
Ilustración 68: Manual de usuario – Crear clave .....	177
Ilustración 69: Manual de usuario – Crear una clave (izquierda); varias claves (derecha)	177



---

Ilustración 70: Manual de usuario – Editar clave .....	178
Ilustración 71: Manual de usuario – Eliminar clave .....	179
Ilustración 72: Manual de usuario – Importar claves.....	179
Ilustración 73: Manual de usuario – Importar claves – Configuración .....	180
Ilustración 74: Manual de usuario – Crear grupo de claves .....	181
Ilustración 75: Manual de usuario – Crear grupo de claves .....	181
Ilustración 76: Manual de usuario – Claves de grupo de claves .....	182
Ilustración 77: Manual de usuario – Editar grupo de claves – Opción menú .....	183
Ilustración 78: Manual de usuario – Editar grupo de claves.....	183
Ilustración 79: Manual de usuario – Eliminar grupo de claves.....	184
Ilustración 80: Manual de usuario – Acceder a escribir .....	185
Ilustración 81: Manual de usuario – Seleccionar tarjeta a escribir .....	185
Ilustración 82: Manual de usuario – Activar tecnología NFC .....	186

## Índice de tablas

Tabla 1:	Valores de TNF.....	16
Tabla 2:	Resumen etiquetas NFC.....	16
Tabla 3:	Formato bits de acceso [45].....	18
Tabla 4:	Operaciones de memoria [45] .....	18
Tabla 5:	Condiciones de acceso para bloque de datos [45] .....	19
Tabla 6:	Condiciones de acceso para bloque cola [45] .....	19
Tabla 7:	Resumen lectores NFC.....	21
Tabla 8:	Conectividad lectores NFC .....	22
Tabla 9:	Lectores NFC compatibles con modo lectura/escritura.....	22
Tabla 10:	Lectores NFC compatibles con modo emulación de tarjeta .....	22
Tabla 11:	Valores SAK de tarjetas RFID .....	25
Tabla 12:	Ejemplo flujo de comunicación Mifare Classic.....	26
Tabla 13:	Formato tabla de requisito de usuario .....	38
Tabla 14:	Requisito RUC-01 – Lectura de tarjetas RFID .....	39
Tabla 15:	Requisito RUC-02 – Selección de claves en lectura .....	39
Tabla 16:	Requisito RUC-03 – Escritura de tarjetas RFID .....	40
Tabla 17:	Requisito RUC-04 – Selección de claves en escritura.....	40
Tabla 18:	Requisito RUC-05 – Gestión de tarjetas RFID .....	40
Tabla 19:	Requisito RUC-06 – Visualización de tarjetas RFID.....	40
Tabla 20:	Requisito RUC-07 – Visualización de condiciones de acceso .....	40
Tabla 21:	Requisito RUC-08 – Importación de tarjetas RFID .....	40
Tabla 22:	Requisito RUC-09 – Estadísticas .....	41
Tabla 23:	Requisito RUC-10 – Gestión de claves.....	41
Tabla 24:	Requisito RUC-11 – Gestión de grupos de claves.....	41
Tabla 25:	Requisito RUC-12 – Importación de claves .....	41
Tabla 26:	Requisito RUC-13 – Activar tecnología NFC .....	41

Tabla 27:	Requisito RUR-01 – Lectura completa.....	42
Tabla 28:	Requisito RUR-02 – Claves para lectura.....	42
Tabla 29:	Requisito RUR-03 – Escritura completa.....	42
Tabla 30:	Requisito RUR-04 – Claves para escritura .....	42
Tabla 31:	Requisito RUR-05 – Cancelación de escritura .....	42
Tabla 32:	Requisito RUR-06 – Tipo de tarjeta en escritura .....	42
Tabla 33:	Requisito RUR-07 – Nombre de tarjeta único .....	43
Tabla 34:	Requisito RUR-08 – Clave única.....	43
Tabla 35:	Requisito RUR-09 – Nombre de grupo de claves único .....	43
Tabla 36:	Requisito RUR-10 – Nombre del tipo de tarjeta único .....	43
Tabla 37:	Requisito RUR-11 – Formato tarjeta Mifare Ultralight.....	43
Tabla 38:	Requisito RUR-12 – Formato tarjeta Mifare Classic Mini .....	43
Tabla 39:	Requisito RUR-13 – Formato tarjeta Mifare Classic 1K .....	44
Tabla 40:	Requisito RUR-14 – Formato tarjeta Mifare Classic 4K .....	44
Tabla 41:	Requisito RUR-15 – Formato clave .....	44
Tabla 42:	Requisito RUR-16 – Longitud clave .....	44
Tabla 43:	Requisito RUR-17 – Tarjeta por tipo .....	44
Tabla 44:	Requisito RUR-18 – Clave por tarjeta .....	44
Tabla 45:	Requisito RUR-19 – Clave por grupo de clave.....	45
Tabla 46:	Requisito RUR-20 – Claves por defecto .....	45
Tabla 47:	Requisito RUR-21 – Tipos de tarjeta por defecto .....	45
Tabla 48:	Requisito RUR-22 – Ruta inicial en importe de tarjetas .....	45
Tabla 49:	Requisito RUR-23 – Ruta inicial en importe de claves .....	45
Tabla 50:	Requisito RUR-24 – Base de datos.....	45
Tabla 51:	Requisito RUR-25 – Backend .....	46
Tabla 52:	Requisito RUR-26 – Lenguaje Android .....	46
Tabla 53:	Requisito RUR-27 – Lenguaje Java .....	46
Tabla 54:	Requisito RUR-28 – Lenguaje SQLite.....	46

Tabla 55:	Requisito RUR-29 – Compatibilidad Android .....	46
Tabla 56:	Requisito RUR-30 – Acceso concurrente al backend.....	46
Tabla 57:	Requisito RUR-31 – Permisos de la aplicación .....	47
Tabla 58:	Requisito RUR-32 – Idioma .....	47
Tabla 59:	Requisito RUR-33 – Conexión a backend.....	47
Tabla 60:	Requisito RUR-34 – Tecnología NFC .....	47
Tabla 61:	Requisito RUR-35 – Aplicación eficiente.....	47
Tabla 62:	Requisito RUR-36 – Aplicación escalable.....	47
Tabla 63:	Requisito RUR-37 – Gestión de fallos.....	48
Tabla 64:	Formato tabla de caso de uso .....	48
Tabla 65:	Caso de Uso CU-01 – Leer tarjeta RFID.....	50
Tabla 66:	Caso de Uso CU-02 – Escribir Tarjeta RFID.....	51
Tabla 67:	Caso de Uso CU-03 – Editar tarjeta RFID .....	52
Tabla 68:	Caso de Uso CU-04 – Crear tarjeta RFID .....	53
Tabla 69:	Caso de Uso CU-05 – Eliminar tarjeta RFID .....	54
Tabla 70:	Caso de Uso CU-06 – Importar tarjetas RFID.....	54
Tabla 71:	Caso de Uso CU-07 – Ver tarjeta en formato ASCII .....	55
Tabla 72:	Caso de Uso CU-08 – Ver tarjeta en formato hexadecimal.....	55
Tabla 73:	Caso de Uso CU-09 – Ver como tarjeta de transporte.....	55
Tabla 74:	Caso de Uso CU-10 – Ver condiciones de acceso .....	56
Tabla 75:	Caso de Uso CU-11 – Ver estadísticas .....	56
Tabla 76:	Caso de Uso CU-12 – Crear clave .....	57
Tabla 77:	Caso de Uso CU-13 – Editar clave .....	57
Tabla 78:	Caso de Uso CU-14 – Eliminar clave.....	58
Tabla 79:	Caso de Uso CU-15 – Crear grupo de claves.....	58
Tabla 80:	Caso de Uso CU-16 – Editar grupo de claves.....	59
Tabla 81:	Caso de Uso CU-17 – Eliminar grupo de claves.....	59
Tabla 82:	Caso de Uso CU-18 – Importar claves .....	60

Tabla 83:	Formato tabla de requisito software .....	60
Tabla 84:	Requisito RSF-01 – Lectura tarjetas Mifare Ultralight .....	62
Tabla 85:	Requisito RSF-02 – Lectura tarjetas Mifare Classic Mini.....	62
Tabla 86:	Requisito RSF-03 – Lectura tarjetas Mifare Classic 1K.....	63
Tabla 87:	Requisito RSF-04 – Lectura tarjetas Mifare Classic 4K.....	63
Tabla 88:	Requisito RSF-05 – Creación de tipos de tarjetas .....	63
Tabla 89:	Requisito RSF-06 – Renombrar tarjeta RFID .....	63
Tabla 90:	Requisito RSF-07 – Reemplazar tarjeta RFID .....	63
Tabla 91:	Requisito RSF-08 – Valor por defecto de bloque .....	64
Tabla 92:	Requisito RSF-09 – Todas las claves para leer tarjetas RFID.....	64
Tabla 93:	Requisito RSF-10 – Grupos de claves para leer tarjetas RFID.....	64
Tabla 94:	Requisito RSF-11 – Ninguna clave para leer tarjetas RFID.....	64
Tabla 95:	Requisito RSF-12 – Escritura tarjetas Mifare Ultralight .....	64
Tabla 96:	Requisito RSF-13 – Escritura tarjetas Mifare Classic Mini .....	65
Tabla 97:	Requisito RSF-14 – Escritura tarjetas Mifare Classic 1K.....	65
Tabla 98:	Requisito RSF-15 – Escritura tarjetas Mifare Classic 4K .....	65
Tabla 99:	Requisito RSF-16 – Todas las claves para escribir tarjetas RFID .....	65
Tabla 100:	Requisito RSF-17 – Grupos de claves para escribir tarjetas RFID.....	65
Tabla 101:	Requisito RSF-18 – Ninguna clave para escribir tarjetas RFID.....	65
Tabla 102:	Requisito RSF-19 – Claves en backend .....	66
Tabla 103:	Requisito RSF-20 – Modificación de tarjetas RFID.....	66
Tabla 104:	Requisito RSF-21 – Borrado de tarjetas RFID .....	66
Tabla 105:	Requisito RSF-22 – Creación de tarjetas Mifare Ultralight .....	66
Tabla 106:	Requisito RSF-23 – Creación de tarjetas Mifare Classic Mini.....	67
Tabla 107:	Requisito RSF-24 – Creación de tarjetas Mifare Classic 1K .....	67
Tabla 108:	Requisito RSF-25 – Creación de tarjetas Mifare Classic 4K.....	67
Tabla 109:	Requisito RSF-26 – Valores por defecto en nuevas tarjetas .....	67
Tabla 110:	Requisito RSF-27 – Visualización en formato ASCII .....	68

Tabla 111:	Requisito RSF-28 – Visualización en formato hexadecimal .....	68
Tabla 112:	Requisito RSF-29 – Visualización como tarjeta de transporte .....	68
Tabla 113:	Requisito RSF-30 – Visualización de condiciones de acceso.....	69
Tabla 114:	Requisito RSF-31 – Importación de una tarjeta RFID .....	69
Tabla 115:	Requisito RSF-32 – Importación de varias tarjetas RFID.....	69
Tabla 116:	Requisito RSF-33 – Almacenamiento de claves en tarjetas importadas....	69
Tabla 117:	Requisito RSF-34 – Ruta importación de tarjetas RFID .....	70
Tabla 118:	Requisito RSF-35 – Estadísticas de uso .....	70
Tabla 119:	Requisito RSF-36 – Creación de claves.....	70
Tabla 120:	Requisito RSF-37 – Creación de varias claves .....	70
Tabla 121:	Requisito RSF-38 – Modificación de claves.....	70
Tabla 122:	Requisito RSF-39 – Eliminación de claves .....	71
Tabla 123:	Requisito RSF-40 – Creación de grupo de claves.....	71
Tabla 124:	Requisito RSF-41 – Modificación de grupo de claves.....	71
Tabla 125:	Requisito RSF-42 – Eliminación de grupo de claves.....	71
Tabla 126:	Requisito RSF-43 – Importación de un fichero de claves .....	71
Tabla 127:	Requisito RSF-44 – Importación de varios ficheros de claves.....	72
Tabla 128:	Requisito RSF-45 – Ruta importación de claves .....	72
Tabla 129:	Requisito RSF-46 – Activación tecnología NFC .....	72
Tabla 130:	Requisito RSF-47 – Prevenir errores.....	72
Tabla 131:	Requisito RSF-48 – Informar de errores.....	72
Tabla 132:	Requisito RSF-49 – Responder ante errores .....	73
Tabla 133:	Requisito RSNF-OP-01 – Tipos de claves .....	73
Tabla 134:	Requisito RSNF-OP-02 – Comprobación al guardar tarjeta.....	73
Tabla 135:	Requisito RSNF-OP-03 – Formato de tarjeta Mifare Ultralight .....	73
Tabla 136:	Requisito RSNF-OP-04 – Formato de tarjeta Mifare Classic Mini.....	74
Tabla 137:	Requisito RSNF-OP-05 – Formato de tarjeta Mifare Classic 1K .....	74
Tabla 138:	Requisito RSNF-OP-06 – Formato de tarjeta Mifare Classic 4K .....	74

Tabla 139:	Requisito RSNF-OP-07 – Comprobación de tipo de tarjeta.....	74
Tabla 140:	Requisito RSNF-OP-08 – Comprobación al guardar clave.....	75
Tabla 141:	Requisito RSNF-OP-09 – Comprobación al guardar grupo de claves .....	75
Tabla 142:	Requisito RSNF-OP-10 – Comprobación al guardar tipo de tarjeta.....	75
Tabla 143:	Requisito RSNF-OP-11 – Activación de tecnología NFC .....	75
Tabla 144:	Requisito RSNF-OP-12 – Ignorar claves en lectura o escritura .....	75
Tabla 145:	Requisito RSNF-OP-13 – Escritura en tarjetas Mifare Ultralight.....	76
Tabla 146:	Requisito RSNF-OP-14 – Lectura y escritura de tarjetas Mifare Classic ....	76
Tabla 147:	Requisito RSNF-OP-15 – Autenticación en tarjetas Mifare Classic .....	76
Tabla 148:	Requisito RSNF-OP-16 – Escritura en tarjetas Mifare Classic .....	76
Tabla 149:	Requisito RSNF-OP-17 – Conexión con tarjeta RFID .....	77
Tabla 150:	Requisito RSNF-OP-18 – Comprobar tipo de tarjeta en operaciones .....	77
Tabla 151:	Requisito RSNF-OP-19 – Claves almacenadas para lectura y escritura .....	77
Tabla 152:	Requisito RSNF-OP-20 – Claves almacenadas para grupos de claves .....	77
Tabla 153:	Requisito RSNF-OP-21 – Grupos de claves almacenados para lectura y escritura .....	77
Tabla 154:	Requisito RSNF-OP-22 – Nombre de ficheros de claves .....	78
Tabla 155:	Requisito RSNF-OP-23 – Nombre de ficheros de tarjetas .....	78
Tabla 156:	Requisito RSNF-OP-24 – Formato de ficheros de claves.....	78
Tabla 157:	Requisito RSNF-OP-25 – Formato de ficheros de tarjetas.....	78
Tabla 158:	Requisito RSNF-OP-26 – Cálculo de estadísticas de uso.....	79
Tabla 159:	Requisito RSNF-OP-27 – Comprobación backend .....	79
Tabla 160:	Requisito RSNF-OP-28 – Búsqueda de tarjetas RFID .....	79
Tabla 161:	Requisito RSNF-OP-29 – Búsqueda de claves.....	79
Tabla 162:	Requisito RSNF-OP-30 – Búsqueda de grupos de claves.....	80
Tabla 163:	Requisito RSNF-OP-31 – Listado de tarjetas .....	80
Tabla 164:	Requisito RSNF-OP-32 – Listado de claves .....	80
Tabla 165:	Requisito RSNF-OP-33 – Notificación de errores .....	80

Tabla 166:	Requisito RSNF-INT-01 – Pantalla principal.....	81
Tabla 167:	Requisito RSNF-INT-02 – Pantalla de selección de claves .....	81
Tabla 168:	Requisito RSNF-INT-03 – Pantalla de espera.....	81
Tabla 169:	Requisito RSNF-INT-04 – Pantalla de lectura/modificación/ver como hexadecimal/nueva tarjeta .....	82
Tabla 170:	Requisito RSNF-INT-05 – Pantalla de ver como ASCII .....	82
Tabla 171:	Requisito RSNF-INT-06 – Pantalla de tarjeta de transporte .....	83
Tabla 172:	Requisito RSNF-INT-07 – Pantalla de condiciones de acceso.....	84
Tabla 173:	Requisito RSNF-INT-08 – Pantalla de tarjetas para escribir .....	84
Tabla 174:	Requisito RSNF-INT-09 – Pantalla de tarjetas RFID .....	85
Tabla 175:	Requisito RSNF-INT-10 – Pantalla de claves y grupos de claves.....	85
Tabla 176:	Requisito RSNF-INT-11 – Pantalla de estadísticas.....	86
Tabla 177:	Requisito RSNF-INT-12 – Diálogo de espera.....	86
Tabla 178:	Requisito RSNF-INT-13 – Diálogo de tarjeta repetida .....	86
Tabla 179:	Requisito RSNF-INT-14 – Diálogo para renombrar tarjeta.....	87
Tabla 180:	Requisito RSNF-INT-15 – Diálogo para eliminar tarjeta.....	87
Tabla 181:	Requisito RSNF-INT-16 – Diálogo para crear tarjeta .....	87
Tabla 182:	Requisito RSNF-INT-17 – Diálogo para crear clave.....	88
Tabla 183:	Requisito RSNF-INT-18 – Diálogo para modificar clave.....	88
Tabla 184:	Requisito RSNF-INT-19 – Diálogo para eliminar clave.....	88
Tabla 185:	Requisito RSNF-INT-20 – Diálogo para crear grupo de claves .....	89
Tabla 186:	Requisito RSNF-INT-21 – Diálogo para modificar grupo de claves.....	89
Tabla 187:	Requisito RSNF-INT-22 – Diálogo para eliminar grupo de claves .....	89
Tabla 188:	Requisito RSNF-INT-23 – Diálogo para importar tarjetas.....	90
Tabla 189:	Requisito RSNF-INT-24 – Diálogo para importar claves.....	90
Tabla 190:	Requisito RSNF-REC-01 – Espacio de almacenamiento .....	90
Tabla 191:	Requisito RSNF-REC-02 – Memoria principal .....	90
Tabla 192:	Requisito RSNF-REC-03 – Velocidad del procesador .....	91



Tabla 193:	Requisito RSNF-REC-04 – Tecnología NFC .....	91
Tabla 194:	Requisito RSNF-REC-05 – Tecnología de red .....	91
Tabla 195:	Requisito RSNF-REN-01 – Tiempos de respuesta .....	91
Tabla 196:	Requisito RSNF-REN-02 – Tiempo de respuesta en primera operación....	91
Tabla 197:	Requisito RSNF-REN-03 – Tiempos de respuesta en Mifare Ultralight.....	92
Tabla 198:	Requisito RSNF-REN-04 – Tiempos de respuesta en Mifare Classic .....	92
Tabla 199:	Matriz de trazabilidad entre requisitos de usuario y requisitos software funcionales .....	95
Tabla 200:	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de operación.....	96
Tabla 201:	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de interfaz.....	97
Tabla 202:	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de recursos.....	98
Tabla 203:	Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de rendimiento.....	98
Tabla 204:	Formato tabla de prueba del sistema .....	106
Tabla 205:	Prueba PSF-01 – Leer tarjeta Mifare Classic Mini .....	107
Tabla 206:	Prueba PSF-02 – Leer tarjeta Mifare Classic 1K.....	107
Tabla 207:	Prueba PSF-03 – Leer tarjeta Mifare Classic 4K.....	108
Tabla 208:	Prueba PSF-04 – Leer tarjeta Mifare Ultralight .....	108
Tabla 209:	Prueba PSF-05 – Escribir tarjeta Mifare Classic Mini .....	109
Tabla 210:	Prueba PSF-06 – Escribir tarjeta Mifare Classic 1K.....	109
Tabla 211:	Prueba PSF-07 – Escribir tarjeta Mifare Classic 4K .....	110
Tabla 212:	Prueba PSF-08 – Escribir tarjeta Mifare Ultralight.....	110
Tabla 213:	Prueba PSF-09 – Crear tarjeta Mifare Classic Mini .....	111
Tabla 214:	Prueba PSF-10 – Crear tarjeta Mifare Classic 1K.....	111
Tabla 215:	Prueba PSF-11 – Crear tarjeta Mifare Classic 4K.....	112
Tabla 216:	Prueba PSF-12 – Crear tarjeta Mifare Ultralight.....	112

Tabla 217:	Prueba PSF-13 – Modificar tarjeta RFID .....	113
Tabla 218:	Prueba PSF-14 – Borrar tarjeta RFID .....	113
Tabla 219:	Prueba PSF-15 – Importar tarjeta Mifare Classic Mini.....	113
Tabla 220:	Prueba PSF-16 – Importar tarjeta Mifare Classic 1K.....	114
Tabla 221:	Prueba PSF-17 – Importar tarjeta Mifare Classic 4K.....	114
Tabla 222:	Prueba PSF-18 – Importar tarjeta Mifare Ultralight .....	115
Tabla 223:	Prueba PSF-19 – Importar varias tarjetas Mifare .....	115
Tabla 224:	Prueba PSF-20 – Crear clave.....	116
Tabla 225:	Prueba PSF-21 – Crear varias claves.....	116
Tabla 226:	Prueba PSF-22 – Modificar clave .....	116
Tabla 227:	Prueba PSF-23 – Eliminar clave .....	117
Tabla 228:	Prueba PSF-24 – Crear grupo de claves.....	117
Tabla 229:	Prueba PSF-25 – Modificar grupo de claves .....	117
Tabla 230:	Prueba PSF-26 – Eliminar grupo de claves .....	118
Tabla 231:	Prueba PSF-27 – Importar un fichero de claves.....	118
Tabla 232:	Prueba PSF-28 – Importar varios ficheros de claves.....	119
Tabla 233:	Prueba PSF-29 – Crear tipo de tarjeta .....	119
Tabla 234:	Prueba PSF-30 – Renombrar tarjeta RFID .....	119
Tabla 235:	Prueba PSF-31 – Reemplazar tarjeta RFID .....	120
Tabla 236:	Prueba PSF-32 – Ver tarjeta RFID en formato ASCII.....	120
Tabla 237:	Prueba PSF-33 – Ver tarjeta RFID en formato hexadecimal.....	120
Tabla 238:	Prueba PSF-34 – Ver tarjeta RFID como tarjeta de transporte .....	120
Tabla 239:	Prueba PSF-35 – Ver condiciones de acceso de una tarjeta RFID .....	121
Tabla 240:	Prueba PSF-36 – Ver estadísticas de uso de las claves.....	121
Tabla 241:	Prueba PSF-37 – Activación tecnología NFC.....	121
Tabla 242:	Matriz de trazabilidad entre requisitos software funcionales y pruebas del sistema.....	123
Tabla 243:	Acrónimos .....	145

---

Tabla 244:	Coste del personal.....	152
Tabla 245:	Coste del equipo.....	152
Tabla 246:	Coste del software.....	153
Tabla 247:	Coste del material fungible.....	153
Tabla 248:	Costes totales .....	154
Tabla 249:	Coste indirectos .....	154
Tabla 250:	Coste del margen de riesgo.....	154
Tabla 251:	Resumen del presupuesto del proyecto .....	154

# CAPÍTULO 1: INTRODUCCIÓN Y OBJETIVOS

## 1. Introducción

Todo lo relacionado con la tecnología, la informática, el internet o saber cómo se utiliza un ordenador, son cuestiones que cada día va cogiendo mayor auge dentro de nuestras vidas, por lo que hay que saber convivir con ello.

Hace unos años, estas áreas no estaban muy desarrolladas pero hoy en día están dentro de nuestras vidas, tan dentro que incluso una cosa tan cotidiana, como es ir a hacer la compra, hoy en día se puede hacer a través de Internet mediante un Smartphone, un ordenador, una tablet o incluso una televisión.

Los dispositivos móviles forman parte de nuestro día a día, de tal forma que tendemos a olvidarnos de que, no hace mucho tiempo, esto no era así. En 1983, con la venta del primer teléfono móvil, nadie se hubiese imaginado que pocos años más tarde existirían más de esos dispositivos. Por aquella época, los teléfonos móviles solo eran poseídos por personas que requerían estar en constante contacto. Años más tarde, con las reducciones de precio y tamaño, estos dispositivos se extendieron rápidamente por todo el mundo.

En el 2007, con la aparición del iPhone, en 2010 la aparición del iPad y finalmente la aparición de smartphones y tables basadas en Android y con un coste menor supuso la popularización de este tipo de dispositivos hasta el punto que en nuestros días la gente suele disponer de al menos uno de estos dos tipos de dispositivos móviles.

Android es un sistema operativo móvil basado en Linux y desarrollado principalmente para dispositivos móviles con pantalla táctil como smartphones y tablets. Fue presentado oficialmente en 2007 y en octubre de 2008 se vendió el primer terminal con sistema operativo Android, HTC Dream. La fundación Open Handset Alliance, liderada por Google, es la encargada de desarrollar Android. [16] [17]

Hoy en día las tecnologías inalámbricas han cobrado gran importancia. Las personas están en constante movimiento y quieren tener la posibilidad de acceder a las redes en todo momento, ya sea para consultar información en internet, para el uso de las redes sociales o para transferencias de archivos e información entre distintos dispositivos sin necesidad de cables que nos limitan la movilidad.

Los dispositivos más utilizados son los teléfonos móviles o Smartphones, los cuales han cambiado tanto su funcionalidad que hoy en día son como un ordenador con tamaño reducido que permiten hacer fotos, vídeos, videollamadas, usarlos como GPS, comunicarse con otros

dispositivos para compartir información mediante tecnologías como Near Field Communication (NFC), WIFI, etc.

NFC es una tecnología basada en identificación por radiofrecuencia que permite la comunicación inalámbrica entre dispositivos que se encuentran a una distancia de hasta 10 cm, intercambiando información a gran velocidad, lo que abre un amplio abanico de aplicaciones atractivas para el usuario, (plataforma de pago, control de acceso, etiquetado de productos, transportes públicos, puntos de información, etc.). [39]

La poca distancia requerida para la conexión entre los dispositivos invita a pensar que existe una intencionalidad consciente por los usuarios cuando ésta se produce. Además, el corto alcance también asegura un nivel de seguridad muy aceptable, ya que es muy difícil que se produzca la comunicación sin intencionalidad o que existan intrusos que intercepten los datos de la comunicación entre dispositivos.

Es por ello que hoy en día se trabaja en desarrollar herramientas que a través de esta tecnología permitan tareas sensibles e importantes como el pago, la identificación personal, el acceso a zonas restringidas, canjeo de descuentos, transferencia de archivos, etc.

Al contrario que otras tecnologías inalámbricas como Wifi o Bluetooth, NFC no está orientada a la transmisión de datos de forma continua y fluida, sino al intercambio rápido de una información puntual, como puede ser la identificación y validación de un usuario o el manejo de datos concretos.

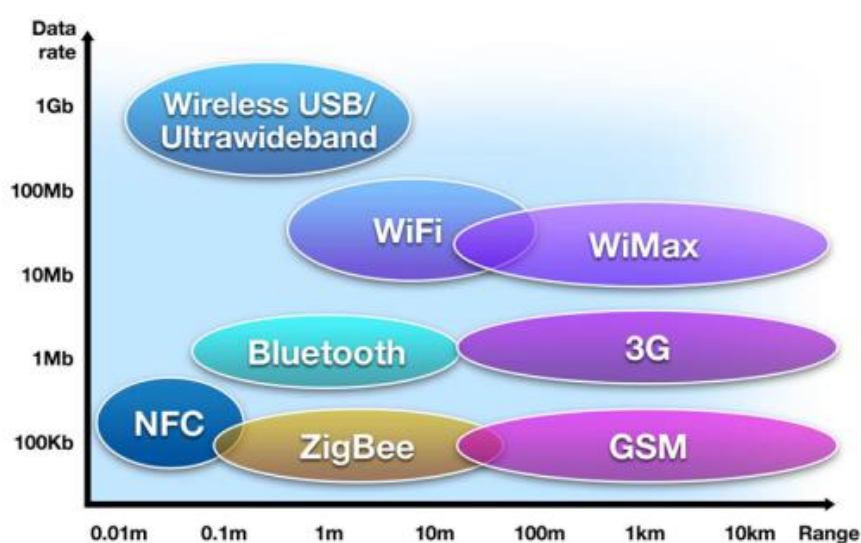


Ilustración 1: NFC vs. otras tecnologías [35]

Google hizo su apuesta por NFC en Android con su versión Gingerbread en el Samsung Nexus S. En un principio fue utilizada para casos de uso sencillo, como son el intercambio de tarjetas personales, pero actualmente ya existen aplicaciones de pago a través de la plataforma de pago Google Wallet [2] .

Cualquier persona, al salir de casa, lleva consigo su teléfono, sus llaves y, probablemente, una cartera. ¿Qué sucedería si se pudiera reemplazar dinero, tarjetas e incluso las llaves gracias al teléfono móvil? En el caso concreto de este proyecto se pretende utilizar la tecnología NFC para que un usuario de Android con tecnología NFC no tenga la necesidad de llevar varias tarjetas RFID consigo, sino que mediante la aplicación Android se pueda identificar, clasificar y almacenar, para posteriormente retransmitirla a través del teléfono sin tener la necesidad de llevar consigo la tarjeta original. Además, se deberán obtener estadísticas de uso sobre las claves y mandarlas a un backend ubicado en Google App Engine.

## 2. Objetivos

El objetivo principal de este proyecto es la creación de una aplicación Android que permita a las personas con dispositivos móviles con tecnología NFC identificar, clasificar, almacenar y retransmitir un número ilimitado de tarjetas RFID.

Para ello antes se necesita comprender bien el problema y plantearse pequeños objetivos que serán necesarios para el buen funcionamiento de la aplicación. Dichos sub-objetivos son:

- Entender y comprender a fondo los conceptos que se van a utilizar, documentándose por medio de Internet en tutoriales, foros, transparencias, etc.

Todos los conceptos a dominar son:

- Tecnología NFC
- Librerías NFC (LibNFC)
- Proxmark3
- Programación SDK Android
- Google App Engine
- Utilizar las librerías NFC para conocer sus capacidades y limitaciones.
- Uso de Proxmark3 para aprender su funcionamiento.
- Diseñar una aplicación en Android compatible con la mayoría de los teléfonos con tecnología NFC que hay en el mercado.

- Utilizar el servicio NFC que ofrece Android en sus terminales móviles para el escaneo, almacenamiento y retransmisión de las tarjetas RFID.
- Diseñar una base de datos que gestione las operaciones sobre las tarjetas RFID almacenadas.
- Desarrollar la aplicación que cumpla con los anteriores criterios.

### 3. Fases del desarrollo

En el presente trabajo existen ocho fases del desarrollo:

1. Documentación e investigación sobre el tema a tratar. Este bloque ha consistido meramente en el asentamiento de las bases del conocimiento para, posteriormente, poder realizar las siguientes fases. La documentación se ha basado en adquirir información global sobre la tecnología NFC, así como ahondar en el uso y la programación del sistema operativo Android. Por otro lado, se ha buscado información sobre otros métodos para el uso de la tecnología NFC, como son los lectores RFID y la Proxmark3.
2. Análisis, donde se ha realizado un estudio del trabajo a realizar, definiendo qué había que hacer y cómo se tenía que hacer en función de los objetivos que hay que cumplir.
3. Configuración del entorno de trabajo, donde se instala y configura todo el hardware y software necesario para la investigación, desarrollo e implementación del proyecto.
4. Desarrollo e implementación de la base de datos, detallando todos aquellos elementos necesarios.
5. Implementación de la aplicación NFC, donde se realiza el desarrollo de las funcionalidades de escritura y lectura NFC para móvil.
6. Integración de la base de datos con las aplicaciones de lectura y escritura NFC, y así completar la funcionalidad del proyecto.
7. Fase de pruebas, donde se ha corroborado que la aplicación realiza todas sus funciones correctamente. Para ello se han contrastado los resultados obtenidos al leer tarjetas RFID en la aplicación desarrollada con los resultados obtenidos al leer las mismas tarjetas con un lector NFC o la Proxmark3.
8. Creación de la presente memoria, que incluye la recopilación de toda la documentación obtenida.



---

## 4. Motivación

Las principales motivaciones para desarrollar este proyecto son:

- Ayudar a cualquier usuario con dispositivo móvil a usarlo como identificación en puntos de control, transportes, etc., mediante el uso de la tecnología NFC.
- Estudio de los mecanismos de seguridad existentes en la tecnología NFC y cómo pueden ser burlados comprometiendo la información de sus usuarios.
- La tecnología NFC ha tenido su auge en su reciente integración en dispositivos móviles, por lo que aún posee una gran posibilidad de usos que han de ser investigados y aprovechados.

En la actualidad los teléfonos inteligentes forman parte de la rutina diaria, por lo que el desarrollo de una aplicación Android con esta tecnología y para dispositivos móviles encaja con la situación a solucionar mejor que una aplicación para PC.

## 5. Estructura del documento

En este apartado se detallará una descripción de la estructura del documento, detallando cada capítulo que se encuentra en el mismo.

En el primer capítulo se ha introducido una visión global de este documento, sus objetivos a cumplir, las fases de desarrollo que se han seguido a lo largo del trabajo realizado, los medios empleados para llevar a cabo este trabajo, y por último, cómo ha sido estructurado este documento para una completa comprensión por parte del lector.

En el segundo capítulo se va a definir el estado del arte, en el cual se comentará el estado actual de la tecnología NFC, en qué consiste su funcionamiento, los tipos de tarjetas RFID que existen, los tipos de lectores RFID que hay para leer dichas tarjetas y los protocolos de encriptación que hay para esta tecnología. Por último, se explicará la situación del sistema operativo Android. Con toda esta información se construirá la base teórica establecida para la creación de este PFC.

En el tercer capítulo se describirá el desarrollo técnico de este trabajo, el cual está dividido en dos partes: análisis y diseño. En el análisis se especifican los requisitos, tanto de usuario como software, y los casos de uso. En la parte de diseño se indica el diagrama de clases junto con la explicación detallada del funcionamiento de cada clase, el diseño de la base de datos utilizado y las interfaces creadas.

En el cuarto capítulo se detallan los experimentos realizados tanto en el dispositivo Samsung Galaxy Nexus como en el PC, comentando al final la comparativa entre las dos pruebas y los resultados aportados.

En el quinto y último apartado se aportarán las conclusiones y futuras líneas de trabajo añadidas por el presente PFC.

## CAPÍTULO 2: ESTADO DEL ARTE

---

En este capítulo se tratará la situación actual de la tecnología empleada para el desarrollo del proyecto, estudios realizados al respecto, y detalles a tener en cuenta para su desarrollo.

## 1. NFC

### 1.1. Introducción

La tecnología NFC trabaja dentro de la banda de radiofrecuencia de los 13,56 MHz, lo que implica que no esté sujeta a ninguna restricción, ni sea necesario disponer de una licencia para su uso por tratarse de una banda libre.

Por tanto, la forma de trabajo de NFC implica que un dispositivo genere una onda de radio de alta frecuencia para que en otro dispositivo NFC, lo suficientemente cercano, se genere un “acoplamiento magnético inductivo”, por medio del cual se puede realizar una transferencia de datos entre dichos dispositivos. El acoplamiento funciona sólo en distancias cortas y es la principal diferencia entre NFC y otras tecnologías inalámbricas como Bluetooth y Wifi, que trabajan a una distancia máxima aproximada de 10m y 100m, respectivamente.

Otra característica significativa de NFC es su compatibilidad con las tecnologías inalámbricas ya existentes como Bluetooth y RFID, lo que hace aún más interesante su uso e incrementa el interés de las empresas en su inversión y desarrollo.

La idea de desarrollar esta tecnología fue crear un nuevo protocolo que preste compatibilidad con las tecnologías sin contacto de corto alcance. Su desarrollo empieza en el año 2002 y sus promotores fueron Philips y Sony principalmente para conseguir compatibilidad con sus tecnologías, Mifare y FeliCa respectivamente, pero fue a finales del año 2003 cuando se aprueba como el estándar ISO 18092.

### 1.1.1. ¿Qué aplicaciones tiene?



Ilustración 2: Aplicaciones NFC

Algunas de las posibles aplicaciones que se pueden desarrollar con esta tecnología son: identificación y control de acceso a espacios controlados, recogida/intercambio de datos, pagos con el teléfono móvil, guía turística, recibir noticias en tiempo real desde un servidor de contenidos, organización de juegos de la búsqueda del tesoro, compra en máquinas expendedoras y control de stocks en comercios.

## 1.2. Características NFC

NFC es un subconjunto de la tecnología RFID y de plataforma abierta que opera sobre la frecuencia 13.56 MHz con un rango de alcance máximo de aproximadamente unos 10 cm.

NFC define tres modos de operación dependiendo del tipo de tag utilizado: activo, semipasivo y pasivo [44] .

- **Activo:** los tags poseen una fuente de alimentación (por lo general una batería) que se utiliza para energizar los circuitos del microchip y transmitir una señal al lector. Como tienen su propia fuente de energía soportan grandes capacidades de memoria y de procesamiento. Son los más costosos.
- **Semipasivo:** los tags utilizan una batería para funcionar los circuitos del microchip pero se comunican mediante el suministro eléctrico proporcionado por el lector. También son costosos.

- **Pasivo:** no poseen fuente de alimentación interna ni para energizar el microchip ni comunicar con el lector, por lo que las capacidades de cálculo y de comunicación son muy limitadas. Sin embargo, en general son capaces de realizar operaciones criptográficas básicas tales como la generación de números pseudoaleatorios y evaluación de funciones pseudoaleatorias.

También define tres modos de configuración entre los dispositivos que desean establecer una comunicación: lectura/escritura, P2P y emulación de tarjeta.

- **Modo Lectura/Escritura:** se da cuando un dispositivo NFC se utiliza en modo activo para emular el comportamiento de un lector de tarjetas de proximidad. La transacción se realiza frente a un objeto pasivo, por ejemplo, una etiqueta o tag, que se comporta como una tarjeta de proximidad.
- **Modo P2P:** hay dos modos:
  - **Activo-Pasivo:** uno de los dos dispositivos, el iniciador, está generando un campo magnético, y el otro dispositivo, el destino o target, lo está recibiendo.
  - **Activo-Activo:** ambos dispositivos, están generando un campo magnético y enviando datos.

Este modo no es recomendado por NFC Forum, es más lento, más complejo y consume más tiempo y batería.

- **Modo emulación de tarjeta:** se da cuando un dispositivo NFC se utiliza en el modo pasivo para emular el comportamiento de una tarjeta de proximidad. La transacción se realiza frente a un dispositivo activo, que emula a un lector de tarjetas de proximidad.

### 1.3. Estandarización

El estándar NFC fue definido por NFC Forum y aprobado como estándar ISO/IEC en diciembre de 2003 y posteriormente como un estándar ECMA. Dicho estándar también está reconocido a nivel Europeo por la ETSI.

Estos estándares especifican:

- Esquemas de modulación, codificación, velocidad de transferencia y formato de la trama de la interfaz de radiofrecuencia de los dispositivos NFC.

- Esquemas de inicialización y condiciones requeridas para el control de colisiones de datos y protocolos de transporte, incluyendo protocolos de activación y métodos de intercambio de datos.

NFC se encuentra estandarizada bajo ISO/IEC 18092/ECMA-340 e ISO/IEC 21481/ECMA-352, e incorpora los estándares ISO/IEC 14443 e ISO/IEC 15693 ya existentes.

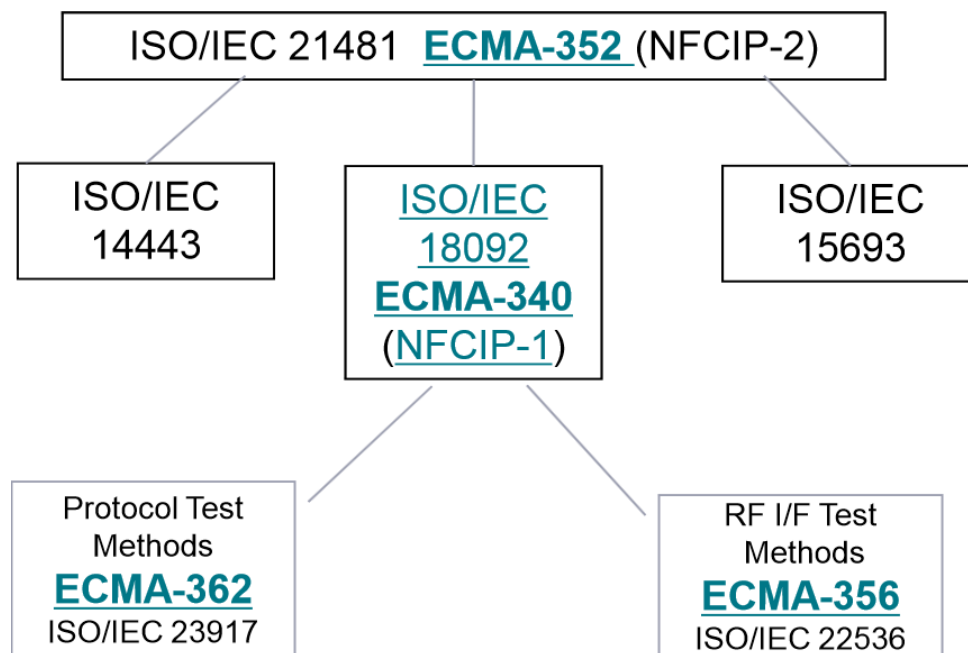


Ilustración 3: Estructura protocolo NFC [41]

- **ISO/IEC 18092/ECMA-340/ETSI TS 102 190 - NFC Interface and Protocol-1 (NFCIP-1):** define el enlace de radio frecuencia con el que NFC opera (13,56 MHz) y los modos de operación activo y pasivo con sus rangos de velocidad desde 106 kbits/s hasta 424 kbits/s.
- **ISO/IEC 21481/ECMA-352/ETSI TS 102 312 - NFC Interface and Protocol-2 (NFCIP-2):** este protocolo especifica los modos de comunicación NFC, PCD (Proximity Coupling Devices) especificado en ISO/IEC 14443, y VCD (Vicinity Coupling Devices) especificado en ISO/IEC 15693.
- **ISO/IEC 14443 Identification cards - Contactless integrated circuit cards – Proximity cards:** define el funcionamiento de las tarjetas de proximidad empleadas para la identificación y los protocolos de transmisión. Este estándar está compuesto de 4 partes: 14443-1 (Características físicas), 14443-2 (Potencia RF Señalización), 14443-3 (Inicialización y Anticolisión) y 14443-4 (Protocolo de transmisión).

- **ISO/IEC 15693 Vicinity Cards:** extiende lo definido en ISO 14443 y aumenta el rango de comunicación.

### 1.3.1. Arquitectura NFC

NFC Forum ha establecido un estándar en el que se define un formato común para poder compartir datos entre dos dispositivos NFC o entre un dispositivo NFC y una etiqueta NFC.

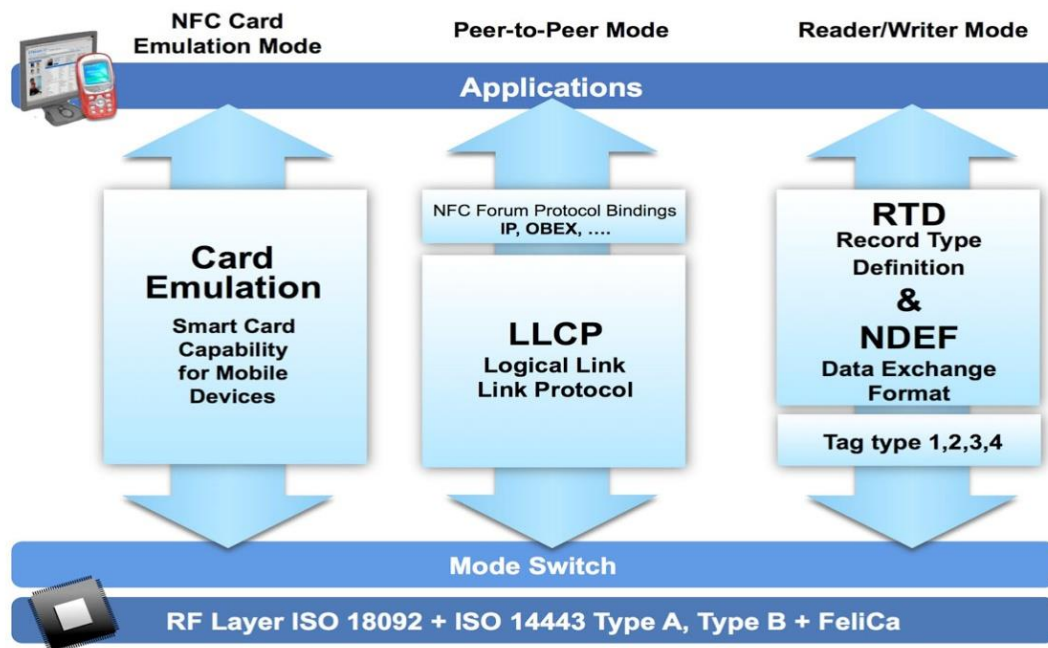


Ilustración 4: Arquitectura NFC

- **NFC Data Exchange Format (NDEF):** especifica un formato común y compacto para el intercambio de datos. NDEF es un formato binario ligero que puede encapsular uno o más payloads (carga útil, es decir, la información útil para el usuario del flujo de información transferido), de diferente tipo y tamaño dentro de la estructura de un solo mensaje. El payload está identificado por un tipo, una longitud y un identificador opcional. El formato de datos de NDEF es el mismo tanto para un dispositivo NFC como para una etiqueta NFC, por lo que la información de NDEF es independiente del tipo de dispositivos que se estén comunicando.
- **NFC Record Type Definition (RTD):** especifica tipos de registros estándar que pueden ser enviados en los mensajes intercambiados entre los dispositivos NFC. Son los que define NFC Forum y que pueden ser incluidos en los mensajes NDEF.
  - **Text RTD:** para registros que sólo contienen texto.



- **Uniform Resource Identifier (URI) RTD:** para registros que se refieren a un recurso de Internet.
- **Smart Poster RTD:** para posters que incorporen etiquetas con datos (URLs, SMSs o números de teléfono).

Un mensaje NDEF contiene uno o varios registros:

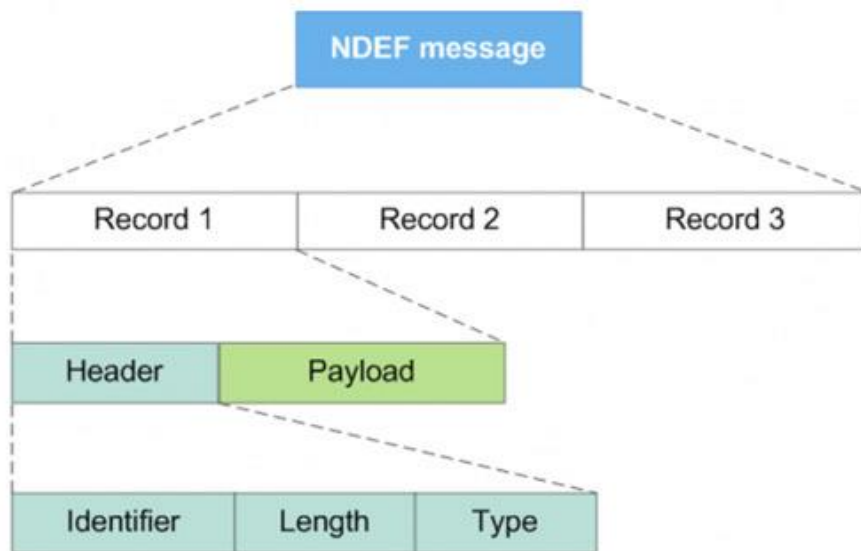


Ilustración 5: Estructura mensaje NDEF [40]

La información de los registros NDEF se presenta en nivel de octetos. El orden de transmisión es de izquierda a derecha y de arriba hacia abajo, por lo que el bit más significativo, al igual que para una cadena de octetos, es el del extremo izquierdo.

Los registros son de longitud variable pero todos tienen el siguiente formato en común:

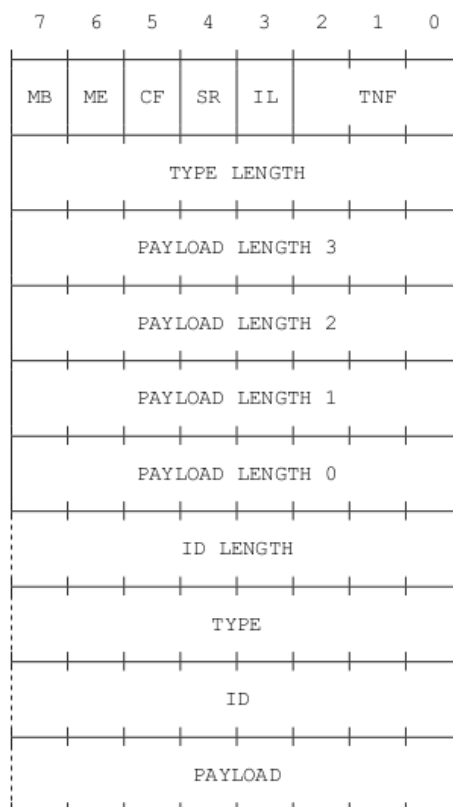


Ilustración 6: Formato registro NDEF [40]

Los campos que lo componen son:

- **MB (Message Begin):** indica que es el primer NDEF Record del mensaje.
- **ME (Message End):** indica que es el último NDEF Record del mensaje.
- **CF (Chunk Flag):** indica que la información se encapsula en varios NDEF Records. Todos los records menos el último deben llevar este flag activado.
- **SR (Short Record):** se utiliza para indicar que la longitud del payload es un octeto (tamaño de payload menor de 255 bytes). Implica la ausencia de PAYLOAD\_LENGTH 3, 2, 1. .
- **IL (ID\_LENGTH):** si el flag está activo, indica que el campo ID\_LENGTH está presente en la cabecera del registro como un octeto, pero si el campo IL es cero entonces éste es omitido de la cabecera y el campo ID también es omitido del registro.
- **TNF (TYPE NAME FORMAT):** es un campo de 3 bits que indica la estructura del valor del campo TYPE. Los valores que puede tener son:

Type Name Format	Valor
Vacio	0x00
Tipo NFC Forum (NFC RTD)	0x01
Tipo de Medios	0x02
URI Absoluto	0x03
Tipo NFC Forum externo	0x04
Tipo Desconocido	0x05
Sin cambio (Unchanged)	0x06
Reservado	0x07

Tabla 1: Valores de TNF

- **ID:** identificador en forma de URI. Sólo el primer registro lleva ID.
- **PAYLOAD:** la estructura interna del payload es transparente para NDEF.

#### 1.4. Etiquetas NFC

Cada etiqueta NFC tiene un código de identificación (ID) único en un rango de 4 a 10 bytes, dependiendo del fabricante de la etiqueta. Todas estas etiquetas se pueden leer/escribir utilizando el formato NDEF.

Resumen de los tipos de etiquetas NFC según NFC Forum y NXP:

	Plataforma NFC Forum				Plataforma NXP
	Tag tipo 1	Tag tipo 2	Tag tipo 3	Tag tipo 4	Tipo Mifare Classic
<b>Productos compatibles</b>	Innovision Topaz	NXP Mifare Ultralight / NXP Mifare Ultralight C	Sony FeliCa	NXP DESFire / NXP SmartMX-JCOP / ISO-14443-A/B	NXP Mifare Classic 1k / NXP Mifare Classic 4k / NXP Mifare Classic Mini
<b>Tamaño memoria</b>	96 B – 2 KB	48 B – 2 KB	1 KB – 1 MB	4 KB / 32 KB	752 B / 3440 B / 224 B
<b>Velocidad de comunicación</b>	106 Kb/s	106 Kb/s	212 Kb/s ó 424 Kb/s	424 Kb/s	106 Kb/s
<b>Precio unitario</b>	Bajo	Bajo	Alto	Medio / Alto	Bajo
<b>Acceso a datos</b>	Lectura/Escritura o solo lectura	Lectura/Escritura o solo lectura	Lectura/Escritura o solo lectura	Lectura/Escritura o solo lectura	Lectura/Escritura o solo lectura
<b>Contenido activo</b>	No	No/No	No	No/Si	No/No/No
<b>Especificaciones de operación</b>	Type 1 Tag	Type 2 Tag	Type 3 Tag	Type 4 Tag	NXP MFTT
<b>Documentación de soporte NXP</b>		NXP T2T		NXP T4T	NXP MFNFC
<b>Fichas de producto NXP</b>		NXP UL, NXP ULC		NXP DES	NXP 1K, NXP 4K, NXP MINI, NXP MAD

Tabla 2: Resumen etiquetas NFC

### 1.4.1. Mifare

Es una tecnología de tarjetas inteligentes sin contacto (TISC). Es equivalente a las 3 primeras partes de la norma ISO-14443-A de 13,56 MHz con protocolo de alto nivel.

Las tarjetas MIFARE son tarjetas de memoria protegida. Están divididas en sectores y bloques y mecanismos simples de seguridad para el control de acceso.

#### 1.4.1.1. Tipos etiquetas Mifare

Fundamentalmente sólo es un dispositivo de almacenamiento de memoria. Hay seis diferentes tipos de tarjetas: Classic, Ultralight, Ultralight C, DESFire, DESFire EV1 y Plus.

- **Mifare Classic:** su memoria se divide en segmentos y bloques con mecanismos de seguridad simples para el control de acceso. Existen tres diferentes tamaños para esta tarjeta: 1K, 4K y Mini. Mifare Classic 1K ofrece 1024 bytes de almacenamiento de datos, divididos en 16 sectores con 4 bloques cada uno. Mifare Classic 4K ofrece 4096 bytes divididos en 40 sectores, de los cuales los 32 primeros tienen el mismo tamaño que los de la tarjeta 1K y los 8 últimos cuatro veces su tamaño. Mifare Classic Mini posee 320 bytes divididos en 5 sectores. Cada sector está protegido por dos claves diferentes llamadas A y B. Estas claves están escritas en 16 bytes reservados en cada sector junto con sus condiciones de acceso. Además, los primeros 16 bytes de la tarjeta son solo de lectura y contiene su identificador, Block Check Character (BCC) e información sobre el fabricante. Según esto la capacidad total disponible que queda para cada tarjeta es 752, 3440 y 224 bytes para Mifare Classic 1K, 4K y Mini, respectivamente. El protocolo de seguridad utilizado es Crypto1.

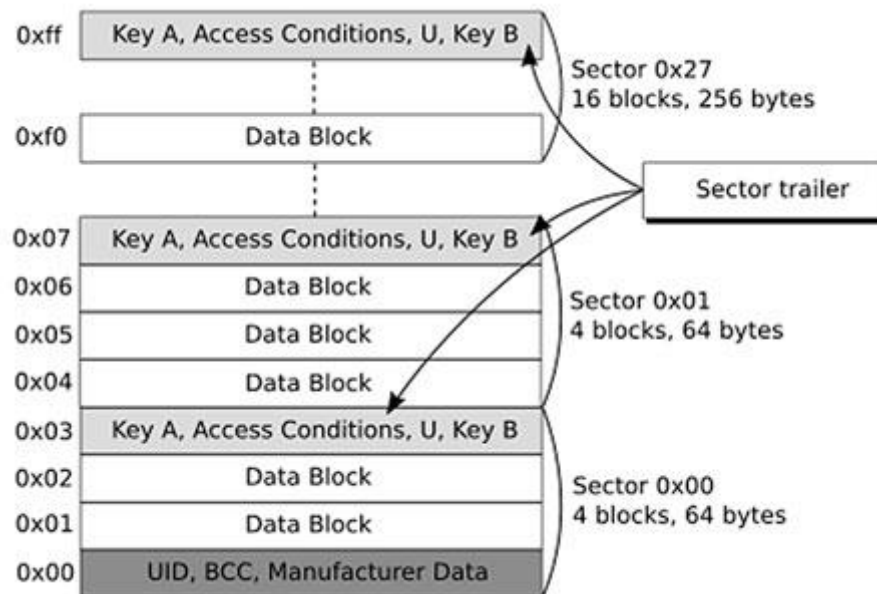


Ilustración 7: Estructura memoria Mifare Classic 4K

Las condiciones de acceso son escritas con el siguiente formato:

Bloque cola

Número byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Clave A					Bytes de acceso				Clave B						

Byte	Bit							
	7	6	5	4	3	2	1	0
6	$\overline{C2}_3$	$\overline{C2}_2$	$\overline{C2}_1$	$\overline{C2}_0$	$\overline{C1}_3$	$\overline{C1}_2$	$\overline{C1}_1$	$\overline{C1}_0$
7	$C1_3$	$C1_2$	$C1_1$	$C1_0$	$\overline{C3}_3$	$\overline{C3}_2$	$\overline{C3}_1$	$\overline{C3}_0$
8	$C3_3$	$C3_2$	$C3_1$	$C3_0$	$C2_3$	$C2_2$	$C2_1$	$C2_0$
9	User Data							

Tabla 3: Formato bits de acceso [47]

El chip de este tipo de tarjetas define las siguientes seis operaciones de memoria que pueden ser usadas para acceder a los bloques de datos:

Operación	Descripción
Lectura	Lee un bloque de datos
Escritura	Escribe un bloque de datos
Incremento	Incrementa el valor y almacena el resultado en el registro de datos interno
Decremento	Decrementa el valor y almacena el resultado en el registro de datos interno
Transferencia	Transfiere el contenido del registro de datos interno a un bloque
Restaurar	Lee el contenido de un bloque del registro de datos interno

Tabla 4: Operaciones de memoria [47]

Los permisos para el uso de estas operaciones están indicados en las condiciones de acceso, así como la clave necesaria para ello.

Las condiciones de acceso están escritas en el bloque cola de cada sector. Existen dos tipos: condiciones de acceso a los bloques de datos y condiciones de acceso al bloque cola, que realizan operaciones sobre los bloques de datos y bloques cola, respectivamente.

○ **Condiciones de acceso para bloque de datos:**

Bits de Acceso			Condición de acceso para			
C1	C2	C3	Lectura	Escritura	Incremento	Decremento, transferencia, restaurar
0	0	0	Clave A B	Clave A B	Clave A B	Clave A B
0	1	0	Clave A B	Nunca	Nunca	Nunca
1	0	0	Clave A B	Clave B	Nunca	Nunca
1	1	0	Clave A B	Clave B	Clave B	Clave A B
0	0	1	Clave A B	Nunca	Nunca	Clave A B
0	1	1	Clave B	Clave B	Nunca	Nunca
1	0	1	Clave B	Nunca	Nunca	Nunca
1	1	1	Nunca	Nunca	Nunca	Nunca

Tabla 5: Condiciones de acceso para bloque de datos [47]

○ **Condiciones de acceso para bloque cola:**

Bits de acceso			Condición de acceso para					
			Clave A		Bits de acceso		Clave B	
C1	C2	C3	Lectura	Escritura	Lectura	Escritura	Lectura	Escritura
0	0	0	Nunca	Clave A	Clave A	Nunca	Clave A	Clave A
0	1	0	Nunca	Nunca	Clave A	Nunca	Clave A	Nunca
1	0	0	Nunca	Clave B	Clave A B	Nunca	Nunca	Clave B
1	1	0	Nunca	Nunca	Clave A B	Nunca	Nunca	Nunca
0	0	1	Nunca	Clave A	Clave A	Clave A	Clave A	Clave A
0	1	1	Nunca	Clave B	Clave A B	Clave B	Nunca	Clave B
1	0	1	Nunca	Nunca	Clave A B	Clave B	Nunca	Nunca
1	1	1	Nunca	Nunca	Clave A B	Nunca	Nunca	Nunca

Tabla 6: Condiciones de acceso para bloque cola [47]

- **Mifare Ultralight:** etiquetas con un tamaño de 64 bytes, divididos en 16 páginas de 4 bytes cada una. No poseen ninguna seguridad criptográfica. Solamente posee las características básicas de seguridad como el bit one-time-programmable (OTP) y el bloqueo de escritura.

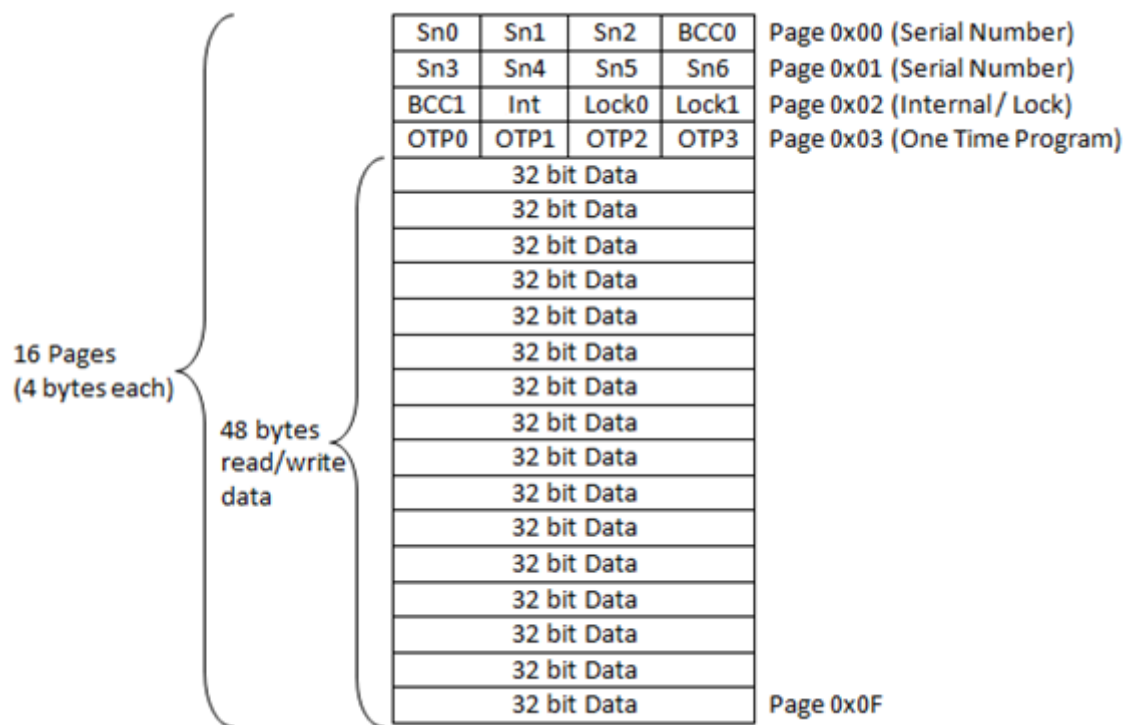


Ilustración 8: Estructura memoria Mifare Ultralight

- **Mifare Ultralight C:** utiliza el algoritmo de seguridad Triple Data Encryption Standard (DES), que es una medida de seguridad contra la clonación. Posee un estándar ampliamente adoptado, lo que permite una fácil integración en las infraestructuras existentes. Sus características principales son:
  - Totalmente compatible con ISO/IEC 14443 1-3 A.
  - 192 bytes de memoria EEPROM.
  - Estructura de memoria como Mifare Ultralight (páginas de 4 bytes).
  - Compatibilidad con versiones anteriores de Mifare Ultralight.
  - Identificador único (UID) de 7 bytes.
- **Mifare DESFire:** con mayor seguridad que Mifare Classic tanto en hardware como en software. Viene preprogramado con un sistema operativo que ofrece una simple estructura de directorios y archivos. Hay cuatro tipos: una con Triple DES y 4KBytes de memoria de almacenamiento, y tres con Advanced Encryption Standard (AES) y una memoria de 2, 4 u 8 KBytes (estas 3 tienen características de seguridad adicionales). Estas tarjetas utilizan un protocolo compatible con ISO/IEC 14443-4.
- **Mifare DESFire EV1 (DESFire8):** evolución de las etiquetas Mifare DESFire. 2, 4 y 8 Kbytes de memoria NV. Alcanza la certificación Evaluation Assurance Level (EAL) 4+, soporta ID aleatorio y cifrado AES de 128 bits.

- **Mifare Plus:** reemplazo para Mifare Classic. Proporciona las mismas funcionalidades que Mifare Classic pero con una mayor seguridad. Sus características son:
  - 2 y 4 Kbytes de memoria.
  - 4 o 7 bytes para UID, con soporte opcional de UID aleatorio.
  - Soporta AES de 128 bits.
  - Obtiene la certificación EAL 4+.

### 1.5. Lectores NFC

Aquí se muestra un resumen de los diferentes lectores NFC compatibles con la librería LibNFC, sus hosts de conectividad y la compatibilidad con los modos lectura, escritura y emulación de tarjeta en función del tipo de chip que posea el lector.

Fabricante	Producto	Chip NFC	Host Bus	Dependencias	Driver	Probado	Soporte
<b>Identive (anteriormente SCM)</b>	SCL3710	PN531 v4.2	USB	Libusb	pn53x_usb	Si	Si
	SCL3711	PN533 v2.7	USB	Libusb	pn53x_usb	Si	Si
<b>Sensor ID</b>	Stick ID	PN533 v2.7	USB	Libusb	pn53x_usb	Si	Si
<b>Toppan Forms</b>	TN31CUD001SW	PN531 v4.2	USB	Libusb	pn53x_usb	Si	Si
<b>Snapper</b>	Feeder	PN531 v3.4	USB	Libusb	pn53x_usb	Si	Si
<b>Sony</b>	RC-S360	PN533_Sony	USB	Libusb	pn53x_usb	Si	Limitado
<b>ASK</b>	LoGO	PN533 v2.7	USB	Libusb	pn53x_usb	Si	Limitado
<b>ACS</b>	ACR122U101	PN532 v1.4	USB	PCSC	acri22_pcsc	Si	Limitado
	ACR122U206	PN532 v1.4	USB	PCSC	acri22_pcsc	Si	Limitado
<b>Tikitag</b>	ACR122U102	PN532 v1.4	USB	PCSC	acri22_pcsc	Si	Limitado
<b>Touchatag</b>	ACR122U102	PN532 v1.4	USB	PCSC	acri22_pcsc	Si	Limitado
<b>Identive (anteriormente Arygon)</b>	ADRA-USB	PN531	USB		arygon	Si	Si
	ADRB-USB	PN532 v1.4	USB		arygon	Si	Si
<b>Sony</b>	RC-S330	PN533_Sony	USB	Libusb	pn53x_usb	Si	Limitado
<b>DDS</b>	Desconocido	PN531 v4.2	USB	Libusb	pn53x_usb	Si	Si
	Desconocido	PN533 v2.7	USB	Libusb	pn53x_usb	Si	Si
<b>microBuilder.eu</b>	PN532 NFC Breakout Board	PN532 v1.6	UART		pn532_uart	Si	Si
<b>Identive (anteriormente Arygon)</b>	APDA1UAxx	PN531	UART			No	N/A
	APDA2UAxx	PN531	UART			No	N/A
	APDB1UA33N	PN532 v1.4	UART		pn532_uart	Si	Si
	APDB2UA33	PN532 v1.4	UART		arygon	Si	Si
	APPA1UAxx	PN531	UART			No	N/A
	APPA2UAxx	PN531	UART			No	N/A
	APPB1UAxx	PN532	UART			No	N/A
	APPB2UAxx	PN532	UART			No	N/A
	APPA2USoo	PN531	USB			No	N/A
	APPB2USoo	PN532	USB			No	N/A

Tabla 7: Resumen lectores NFC



### 1.5.1. Conectividad

	PN531	PN532	PN533
UART	Si	Si	No
USB	Si	Si	Si
SPI	Si	Si	No
I <sup>2</sup> C	Si	Si	No

Tabla 8: Conectividad lectores NFC

### 1.5.2. Compatible con modo lectura/escritura

	PN531	PN532	PN533
ISO14443-A	Si (106 kbps)	Si (106 kbps)	Si (106 kbps)
ISO14443-B	No	Si (106 kbps)	Si (106/212/424/847 kbps)
Felica	Si (212/424 kbps)	Si (212/424 kbps)	Si (212/424 kbps)
Jewel/Topaz	No	Si (106 kbps)	Si (106 kbps)
D.E.P.	Si	Si	Si

Tabla 9: Lectores NFC compatibles con modo lectura/escritura

### 1.5.3. Compatible con modo emulación de tarjeta

	PN531	PN532	PN533
ISO14443-3	Si (UID de 4 bytes)	Si (UID de 4 bytes)	Si (UID de 4 bytes)
ISO14443-4	Si (software)	Si (hardware)	Si (software)
ISO14443-B	No	No	No
FeliCa	Si (212/424 kbps)	Si (212/424 kbps)	Si (212/424 kbps)
Jewel/Topaz	No	No	No
D.E.P.	Si	Si	Si

Tabla 10: Lectores NFC compatibles con modo emulación de tarjeta

## 1.6. Flujo de comunicación Mifare Classic

La comunicación realizada por las tarjetas Mifare Classic sigue la parte 3 del estándar ISO-14443-A. Los comandos utilizados para ello son:

<b>Authentication</b>			
READER	CARD	READER	CARD
60 YY* Using KeyA	4-byte nonce	8-byte response	4-byte response
61 YY* Using KeyB	4-byte nonce	8-byte response	4-byte response
<b>Data</b>			
READER	CARD	READER	
30 YY* Read	16 data bytes*		
A0 YY* Write	ACK / NACK	16 data bytes*	
<b>Value blocks</b>			
READER	CARD	READER	READER
C0 YY* Decrement	ACK / NACK	4-byte value*	Transfer
C1 YY* Increment	ACK / NACK	4-byte value*	Transfer
C2 YY* Restore	ACK / NACK	4-byte value*	Transfer
B0 YY* Transfer	ACK / NACK		
<b>Other</b>			
READER			
50 00* Halt			

YY = block address  
 \* = Followed by two CRC bytes

<b>Card responses (ACK / NACK)</b>	
A (1010)	ACK
4 (0100)	NACK, not allowed
5 (0101)	NACK, transmission error

Ilustración 9: Comandos Mifare Classic

A continuación se muestra una imagen donde se puede observar las etapas que componen la comunicación, y posteriormente una explicación del funcionamiento de cada una. [49]

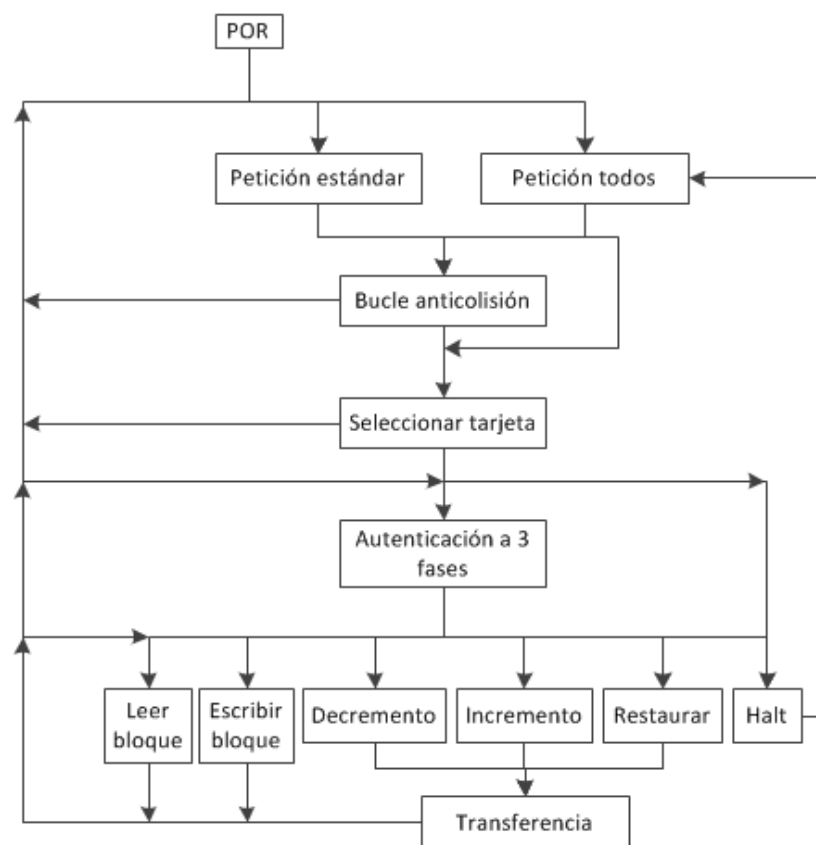


Ilustración 10: Flujo de comunicación Mifare Classic

### 1.6.1. Solicitud estándar/Solicitud todos

La tarjeta RFID se encuentra inicialmente en el estado Power On Reset (POR) debido a que no está interactuando con ningún campo electromagnético. Con el fin de detectar las tarjetas en dicho campo el lector RFID envía repetidamente el comando REQuest Type A (REQA, 26) o Wake UP Type A (WUPA, 52). Este último comando despertará todas las tarjetas en los estados POR y HALT. Cuando una tarjeta está dentro del rango del campo del lector responde a la petición con el comando Answer To reQuest Type A (ATQA). En este momento el lector reconoce que al menos hay una tarjeta en el rango de lectura y comienza con el bucle anticolisión.

### 1.6.2. Bucle anticolisión

Esta etapa puede desarrollarse de dos maneras: con una o con varias tarjetas dentro del rango del campo del lector.

- **Una tarjeta:** el lector obtiene el UID de la tarjeta con el comando Anticollision Command (AC, 93 20) y el bucle termina.
- **Varias tarjetas:** esta situación se produce debido a una colisión cuando dos tarjetas transmiten simultáneamente patrones de bits donde una o más posiciones de bit poseen valores complementarios. El lector tiene en cuenta solo la información válida hasta el bit de colisión estableciéndola como el nuevo criterio de búsqueda. Envía otro comando AC actualizado con el nuevo criterio y la longitud. La tarjeta cuyo UID coincida con el nuevo criterio responderá. Este proceso se repite hasta que no haya colisiones y las tarjetas RFID no seleccionadas entran en modo de espera hasta una nueva petición por parte del lector.

### 1.6.3. Seleccionar tarjeta

El lector envía el comando Select card (SEL, 93 70) a la tarjeta seleccionada para la autenticación y posteriores accesos de memoria. La tarjeta responderá con el comando Select AcKnowledge (SAK). El SAK y los mensajes ATQA también determinan el tipo de tarjeta y el nombre del fabricante.

A continuación se muestra algunos valores SAK y ATQA conocidos.

Fabricante	Producto	ATQA	1º byte SAK (hexadecimal)
NXP	MIFARE Mini	04 00	09
	MIFARE Classic 1K	04 00	08
	MIFARE Classic 4K	02 00	18
	MIFARE Ultralight	44 00	00
	MIFARE DESFire	44 03	20
	MIFARE DESFIRE EV1	44 03	20
	JCOP <sub>31</sub>	04 03	28
	JCOP <sub>31</sub> v2.4.1	48 00	20
	JCOP <sub>41</sub> v2.2	48 00	20
	JCOP <sub>41</sub> v2.3.1	04 00	28
Infineon	MIFARE Classic 1K	04 00	88
Gemplus	MPCOS	02 00	98

Tabla 11: Valores SAK de tarjetas RFID

#### 1.6.4. Autenticación a tres fases

Esta etapa realiza la autenticación entre la tarjeta y el lector en tres fases de desafío-respuesta, donde la respuesta es la salida de una función de transformación que tiene el desafío como la entrada, y se envía encriptada con la clave secreta. Las tres fases en Mifare Classic son las siguientes:

- **Fase 1:** el lector ha solicitado el acceso a algún bloque y la tarjeta envía un número aleatorio de 4 bytes al lector ( $n_T$ ).
- **Fase 2:** el lector responde con su propio número aleatorio ( $n_R$ ) encriptado y una respuesta cifrada ( $a_R$ ) al desafío de la fase 1. Desde este mensaje en adelante toda la comunicación es encriptada.
- **Fase 3:** si la respuesta del lector es correcta la tarjeta responderá con una respuesta cifrada ( $a_T$ ), sino no responderá y el flujo de comunicación habrá terminado.

Al final de esta autenticación ambas partes pueden descifrar y verificar la exactitud de las respuestas, y están seguros de que la otra parte posee la clave correcta.

#### 1.6.5. Halt

En cualquier momento después de que una tarjeta ha sido seleccionada por el lector este puede cesar toda la comunicación con ella mediante la emisión del comando HALT Type A (HLTA). La tarjeta se situará en el estado de pausa y solo puede ser despertada con el comando WUPA.

A continuación se muestra un ejemplo de flujo de comunicación:

Etapa	Secuencia	Emisor	Bytes (hexadecimal)	Comando
Solicitud estándar	1	Lector	26	REQA (WUPA si es 52)
	2	Tarjeta	04 00	ATQA
Bucle anticolidión	3	Lector	93 20	AC
	4	Tarjeta	2A 69 8D 43 8D	UID y BCC
Seleccionar tarjeta	5	Lector	93 70 2A 69 8D 43 8D 52 55	SEL
	6	Tarjeta	08 B6 DD	SAK
Autenticación a tres fases	7	Lector	60 04 D1 3D	Autenticación bloque 0x04 con clave A
	8	Tarjeta	3B AE 03 2D	Aleatorio de tarjeta
	9	Lector	C4 94 A1 D2 6E 96 86 42	Aleatorio y respuesta de lector cifrados
	10	Tarjeta	84 66 05 9E	Respuesta de tarjeta cifrada
Halt	11	Lector	50 00 57 CD	HLTA

Tabla 12: Ejemplo flujo de comunicación Mifare Classic

## 1.7. Crypto1

Crypto1 es un algoritmo de cifrado desarrollado por NXP Semiconductors específicamente para su uso en tarjetas MIFARE Classic. El algoritmo se ejecuta en el hardware del chip de estas tarjetas para las operaciones criptográficas rápidas. [42] [43] [45] [46] [50]

### 1.7.1. Cifrado de flujo

Crypto1 es un cifrado basado en un Linear Feedback Shift Register (LFSR) de 48 bits y un generador de filtro no lineal de dos capas ( $f_a$ ,  $f_b$  y  $f_c$ ). El polinomio generador del LFSR ( $g(x) = x^{43} + x^{42} + x^{41} + x^{39} + x^{35} + x^{29} + x^{27} + x^{25} + x^{24} + x^{19} + x^{17} + x^{15} + x^{14} + x^{12} + x^{10} + x^9 + x^5 + 1$ ) es primitivo por lo que es irreducible y genera los  $2^{48} - 1$  estados antes de volver a generar el estado inicial.

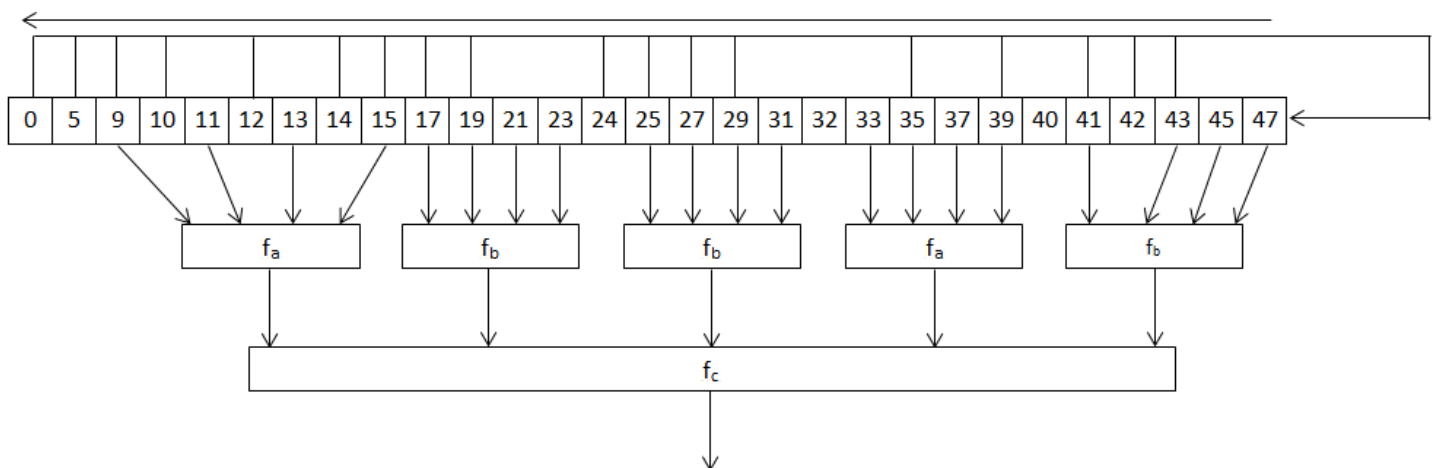


Ilustración 11: Crypto1 – Estructura cifrado de flujo

#### 1.7.1.1. Generador de clave

Durante cada ciclo de reloj el LFSR realiza el siguiente procedimiento para que el generador de filtro no lineal recolecte veinte bits y genere un nuevo bit de clave:

- 1) Genera nuevo bit utilizando la función de realimentación.
- 2) El LFSR se desplaza un bit a la izquierda descartando el bit más a la izquierda.
- 3) Inserta a la derecha el bit generado en el paso 1.

Si usamos  $x_n$  para denotar el valor del bit (0 ó 1) en la posición  $n$  y es la función exclusiva or (XOR) lógica la función de realimentación se define entonces por:

$$L(x_0x_1 \dots x_{47}) := x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \\ \oplus x_{29} \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43}$$

El generador de filtro genera un bit en cada ciclo de reloj y se puede definir como una combinación de tres subfunciones lógicas:  $f_a$ ,  $f_b$  y  $f_c$ . Utilizando la misma notación  $x_n$  que el anterior e introduciendo los operadores lógicos OR ( $\vee$ ) y AND ( $\wedge$ ) se define el generador de filtro y los tres sub-funciones así:

$$f(x_0x_1 \dots x_{47}) := f_c(f_a(x_9, x_{11}, x_{13}, x_{15}), f_b(x_{17}, x_{19}, x_{21}, x_{23}), f_b(x_{25}, x_{27}, x_{29}, x_{31}), \\ f_a(x_{33}, x_{35}, x_{37}, x_{39}), f_b(x_{41}, x_{43}, x_{45}, x_{47}))$$

Donde:

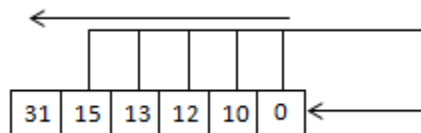
$$f_a(a, b, c, d) := ((a \vee b) \oplus (a \wedge d)) \oplus (c \wedge ((a \oplus b) \vee b))$$

$$f_b(a, b, c, d) := ((a \wedge b) \vee c) \oplus ((a \oplus b) \wedge (c \vee d))$$

$$f_c(a, b, c, d, e) := (a \vee ((b \vee e) \wedge (d \oplus e))) \oplus ((a \oplus (b \wedge d)) \wedge ((c \oplus d) \vee (b \wedge e)))$$

### 1.7.2. Generador de números pseudoaleatorios

Es un circuito encargado de generar números pseudoaleatorios (RNG) de 32 bits basado en un LFSR de 16 bits con el polinomio generador  $g(x) = x^{16} + x^{14} + x^{13} + x^{11} + 1$  y separado del LFSR de 48 bits utilizado para el cifrado.



**Ilustración 12: Crypto1 – Estructura del generador de números pseudoaleatorios**

Utiliza el mismo procedimiento que el LFSR del cifrado para generar un bit de salida.

Denotando la función de realimentación de la misma manera queda definida como:

$$L(x_0x_1 \dots x_{15}) := x_0 \oplus x_{11} \oplus x_{13} \oplus x_{14} \oplus x_{16}$$

Por otra parte, si se define la secuencia  $x_0x_1\dots x_{31}$  de un LFSR de 32 bits que consiste en este LFSR de 16 bits la siguiente secuencia de 32 bits se puede definir mediante una función sucesor donde:

$$suc(x_0x_1 \dots x_{31}) := x_1x_2 \dots x_{31}L(x_{16}x_{17} \dots x_{31})$$

$$suc^n(x_0x_1 \dots x_{31}) := suc^{n-1}(suc(x_0x_1 \dots x_{31}))$$

### 1.7.3. Flujo interno del algoritmo Crypto1

La ejecución interna que realiza el algoritmo Crypto1 consiste en dos etapas: inicialización y encriptación. [42] , [43] , [45] , [46] , [50]

#### 1.7.3.1. Inicialización

En este proceso se inician los valores del LFSR del generador de claves y el LFSR del RNG con la clave del sector a autenticar y el número aleatorio mandado al lector en la fase 1 en la autenticación a tres fases, respectivamente.

A continuación el contenido del LFSR del generador de claves es desplazado con el resultado de la operación  $uid \oplus n_T$  (operación XOR entre el identificador de la tarjeta y el número aleatorio de la tarjeta). Por último es desplazado con el número aleatorio enviado por el lector en la fase 2 en la autenticación a tres fases.

#### 1.7.3.2. Encriptación

Una vez que la inicialización ha terminado comienza el encriptado. Para llevarlo a cabo se realizan los siguientes pasos:

1. Los bits en las posiciones 9,11,13 y 15, 17,19,21 y 23, 25,27,29 y 31, 33,35,37 y 39, y 41,43,45 y 47 son extraídos del generador de claves y suministrados a las funciones  $f_a, f_b, f_b, f_a$  y  $f_b$ , respectivamente.
2.  $f_a$  y  $f_b$  son calculadas.
3. Los resultados de estas 5 funciones son insertados en la función  $f_c$ .
4.  $f_c$  es calculada.
5. El LFSR de RNG es desplazado una posición a la izquierda.
6. Se realiza la operación XOR con los bits de las posiciones 0, 10, 12, 13 y 15 del RNG.
7. El resultado del paso 6 es insertado en el LFSR de RNG.
8. Operación XOR entre los valores obtenidos en los pasos 4 y 6. El resultado obtenido es un bit perteneciente al resultado final.

9. El LFSR del generador de claves es desplazado una posición a la izquierda.
10. Se realiza la operación XOR entre los bits de las posiciones 0, 5, 9, 10, 12, 14, 15, 17, 19, 24, 25, 27, 29, 35, 39, 41, 42 y 43 del generador de claves.
11. Operación XOR entre el valor obtenido en el paso 4 y el número aleatorio enviado por el lector.
12. Operación XOR entre el valor obtenido en el paso 11 y el resultado de la operación XOR entre el identificador de la tarjeta y el número aleatorio enviado al lector.
13. Operación XOR entre los valores obtenidos en los pasos 10 y 12.
14. El resultado del paso 13 es insertado en el LFSR de generador de claves.
15. Volver a ejecutar el paso 1.

Según todo lo anterior, la estructura completa del algoritmo Crypto1 es:

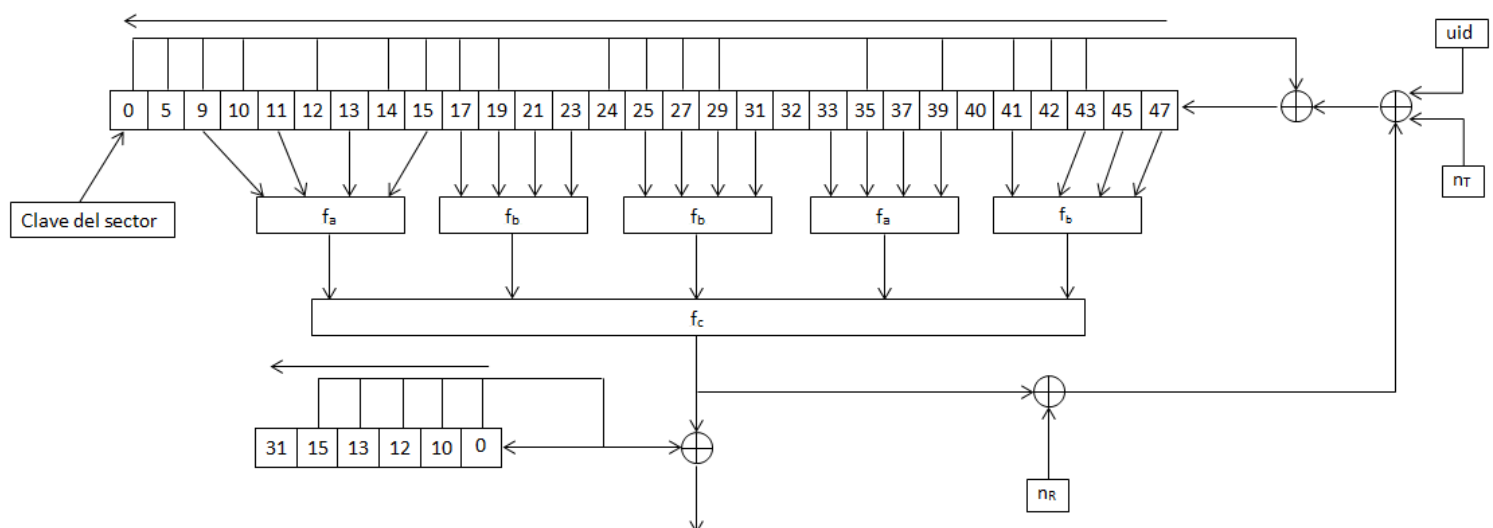


Ilustración 13: Crypto1 – Estructura completa

## 1.8. Herramientas de ataque NFC

### 1.8.1. Proxmark3

Proxmark3 posee un programa cliente con el que el usuario puede interactuar con el dispositivo permitiéndole espiar, escuchar y emular tarjetas RFID tanto de baja como de alta frecuencia. Su desarrollo ha sido en sistemas Unix pero existen versiones para sistemas operativos como Windows [49] .

Este programa posee diferentes funciones para operar sobre las tarjetas RFID, a continuación se especifican las utilizadas para el desarrollo de este proyecto: [21]



- **hf 14a list:** muestra los mensajes intercambiados previamente entre una tarjeta RFID y la proxmark3 o desde una ejecución previa del comando hf 14a snoop.
- **hf 14a reader:** emplea el proceso de anticolisión sobre una tarjeta RFID y muestra la información recolectada de sus respuestas.
- **hf 14a snoop:** registra todo el tráfico de información entre el lector y la tarjeta RFID. Todo este tráfico puede ser mostrado con el comando hf 14a snoop.
- **hf mf mifare:** obtiene la clave del bloque o.
- **hf mf nested:** obtiene las claves de uno o todos los sectores de una tarjeta RFID, pudiendo escoger entre obtener las claves tipo A, B o ambas. Para poder ejecutarlo es necesario conocer al menos una clave.
- **hf mf sim:** emula el comportamiento de una tarjeta Mifare Classic.
- **hf mf eclr:** limpia la memoria de la Proxmark3 y la rellena con la clave por defecto (0xFFFFFFFFFFFFFFFF).
- **hf mf ekeyprn:** muestra las claves almacenadas en la memoria de la Proxmark3.

### 1.8.2. LibNFC

El propósito de la biblioteca libnfc es proporcionar a los desarrolladores una manera de trabajar con hardware NFC a un nivel más alto de abstracción sin costo alguno. Algunas funciones importantes incluyen soporte para ISO-14443-A modulación, implementación del protocolo MIFARE Classic y la capacidad de transformar cualquier dispositivo NFC basada en USB en un lector o tarjeta RFID. A continuación se destacan aquellos que se han utilizado directamente: [26] , [49]

- **nfc-anticol:** genera una fase de anticolisión para el estándar ISO14443-A.
- **nfc-emulate-tag:** emula un tag.
- **nfc-emulate-uid:** emula un tag que posee un UID modificado.
- **nfc-list:** lista la primera tarjeta RFID actual de cada lector.
- **nfc-mfclassic:** manipulación de una tarjeta Mifare Classic.
- **nfc-mfultralight:** manipulación de una tarjeta Mifare Ultralight.
- **nfc-scan-device:** lista los dispositivos NFC disponibles.

### 1.8.3. Crapto1

Crapto1 es una librería escrita en lenguaje C que además de implementar el cifrado Crapto1 ofrece algunas funciones de ataque contra él. [30] , [42] , [49]

En este proyecto Crapto1 es utilizado para realizar ingeniería inversa sobre el algoritmo Crypto1 y así descifrar las claves de las tarjetas RFID de tipo Mifare Classic.

Los valores utilizados para el cifrado son el uid, aleatorio y la clave del sector de la tarjeta. Ya que todos son conocidos excepto la clave, y debido a la propiedad:

$$C = A \oplus B$$

Entonces:

$$A = B \oplus C$$

$$B = A \oplus C$$

Es posible realizar el procedimiento inverso comenzando desde el último resultado encriptado y así obtener la clave del sector.

Esta librería está incluida en el programa Mfoc, el cual es utilizado para descifrar las claves de las tarjetas RFID de tipo Mifare Classic durante el desarrollo de este proyecto.

## 2. Android

### 2.1. Introducción

#### 2.1.1. ¿Qué es Android?

Andy Rubin define Android como:

*“La primera plataforma verdaderamente abierta y global para dispositivos móviles, con todo el software para hacer funcionar un teléfono móvil pero sin los obstáculos de los propietarios que han entorpecido la innovación en el mundo de los dispositivos móviles.” [34]*

Android es un software de código abierto que incluye un sistema operativo, un middleware o capa intermedia, las principales aplicaciones móviles necesarias para cualquier dispositivo móvil y un conjunto de librerías que permiten escribir nuevas aplicaciones que se podrán instalar en dispositivos móviles que tengan Android instalado. Además, Android se ha diseñado de forma que tanto las aplicaciones nativas del software como las aplicaciones desarrolladas por terceras personas estén escritas bajo las mismas APIs y funcionen bajo el mismo entorno de ejecución.

Desde su aparición en 2008 han salido numerosas actualizaciones. Éstas corrigen fallos, implementan nuevas funcionalidades, mejoran el rendimiento, etc. Las aplicaciones desarrolladas son por regla general retrocompatibles.

Las diferentes versiones que hay son:



Ilustración 14: Versiones de Android

Para el desarrollo de este proyecto se ha utilizado la versión 4.0.4 (Ice Cream Sandwich):

- Basado en el núcleo de Linux 3.0.1.
- Habilidad de acceder a aplicaciones directamente desde la pantalla de bloqueo.
- Mejor integración de voz y dictado de texto en tiempo real continuo.
- Desbloqueo facial, característica que permite a los usuarios desbloquear los equipos usando software de reconocimiento facial.
- Nuevo navegador web con pestañas bajo la marca de Google Chrome, permitiendo hasta 15 pestañas.
- Capacidad para cerrar aplicaciones que están usando datos en segundo plano.
- Editor de fotos integrado.
- Android Beam, una característica de NFC que permite el rápido intercambio de datos a corto alcance.
- Aceleración por hardware de la interfaz de usuario.

## 2.2. Arquitectura

El sistema operativo Android posee una arquitectura con estructura multicapa formada por cinco capas. Cada una de estas capas utiliza elementos de la capa inferior para realizar sus funciones.

Las capas que lo componen son:

- **Kernel de Linux:** Android se basa en la versión 2.6 del kernel de Linux para los servicios básicos del sistema como seguridad, gestión de memoria y procesos, conexiones de red y montaje de drivers. También actúa como una capa de abstracción entre el hardware y el resto de las capas de la arquitectura.
- **Librerías:** la capa que se sitúa justo sobre el kernel la componen las librerías nativas de Android. Estas librerías están escritas en C/C++ y compiladas para la arquitectura hardware específica del teléfono, tarea que normalmente realiza el fabricante y que también se encarga de instalarlas en el terminal antes de ponerlo a la venta. Su cometido es proporcionar funcionalidad a las aplicaciones, para tareas que se repiten con frecuencia, evitando tener que codificarlas cada vez y garantizando que se llevan a cabo de la forma más eficiente.

Algunas de las librerías son: Surface Manager, SGL, OpenGL, Media Framework, WebKit, SSL, FreeType, SQLite y la librería C del sistema (libc).

- **Entorno de ejecución:** Android incluye un conjunto de librerías básicas que proporcionan la mayor parte de la funcionalidad disponible en las librerías de Java. Además, Android dispone de una máquina virtual similar a la que dispone el lenguaje Java, que ha sido rediseñada de forma que cuando un proceso es lanzado a ejecución disponga de su propia instancia de máquina virtual. Así, un dispositivo móvil puede tener en un momento dado múltiples instancias de máquinas virtuales ejecutándose en paralelo, gestionándolas todas de forma eficiente y equilibrada en términos de consumo de memoria. Dicha máquina virtual se conoce bajo el nombre de Dalvik.
- **Framework de aplicaciones:** mediante este nivel, los desarrolladores tienen acceso a los dispositivos hardware del terminal, pueden ejecutar servicios en segundo plano, activar alarmas, y todo lo necesario para implementar aplicaciones de gran potencia. Para ello, se les da un acceso total al mismo API que se utiliza para el desarrollo de las aplicaciones básicas del nivel aplicaciones. De esta forma se favorece la reutilización de los componentes, y se posibilita el hecho de poder cambiar componentes a gusto del usuario.
- **Aplicaciones:** capa superior de la arquitectura. La forman las aplicaciones del dispositivo: con interfaz de usuario o sin ella, nativas (C/C++) o administradas (Java), instaladas de serie con el dispositivo por el fabricante o instaladas a posteriori por el usuario.

### 2.3. NFC en Android

Con la versión 2.3 comienza el soporte de NFC sobre Android. Pero la API facilitada a los desarrolladores no permite aprovechar todas las capacidades que NFC puede ofrecer, por lo que en poco espacio de tiempo Google lanzó una versión mejorada. Esta nueva versión mejoró el soporte de tarjetas y añadió la posibilidad de enviar mensajes NDEF entre teléfonos.

Las posibilidades que ofrece Android para trabajar con NFC son las siguientes:

- Lectura escritura de diferentes tipos de tarjeta: todas las posibles tarjetas están representadas por la clase *Tag*. Las propiedades de esta permiten obtener el tipo de tarjeta aproximada y en función de la que sea obtener la clase que la representa ese tipo. En el paquete *android.nfc.tech* se encuentran las clases disponibles, que ofrecen soporte para los siguientes tipos de tarjeta: NFC-A (ISO 14443-3A), NFC-B (ISO 14443-3B), NFC-F (JIS 6319-4), NFC-V (ISO 15693), ISO-DEP (ISO 14443-4), MIFARE Classic, MIFARE Ultralight y NFC Forum NDEF tags.
- Formateado de diferentes mensajes NDEF: permite trabajar a alto nivel con los diferentes tipos de mensajes NDEF (texto, URL...) tanto en la lectura como en la escritura.
- Posibilidad de intercambiar mensajes NDEF entre teléfonos móviles: a modo de conexión peer to peer, se pueden enviar o recibir mensajes NDEF como si de una tarjeta se tratase.
- Aviso de aproximación de un elemento NFC: cuando se aproxima una tarjeta u otro móvil, se puede preparar para que la aplicación que este en primer plano reciba el correspondiente aviso, con un Intent (como suele trabajarse en Android, a modo de "Evento") o se puede configurar para elegir que aplicación se abrirá por defecto en caso de no estar ejecutándose ninguna aplicación relacionada.
- Android 4.4 permite realizar transacciones seguras con NFC a través de Host Card Emulation (HCE), el cual emula la norma ISO/IEC 7816 basado en tarjetas inteligentes que utilizan el protocolo ISO/IEC 14443-4 (ISO-DEP).

## 3. SQLite

SQLite es un sistema de gestión de bases de datos relacional de dominio público y compatible con ACID (Atómica, consistente, aislada y durable), contenida en una biblioteca relativamente pequeña (~275 Kb) y escrita en C.

A diferencia de los sistemas de gestión de bases de datos cliente-servidor, el motor de SQLite no es un proceso independiente con el que el programa principal se comunica. En lugar de eso, la biblioteca SQLite se enlaza con el programa pasando a ser parte integral del mismo. El programa utiliza la funcionalidad de SQLite a través de llamadas simples a subrutinas y funciones. Esto reduce la latencia en el acceso a la base de datos, debido a que las llamadas a funciones son más eficientes que la comunicación entre procesos. El conjunto de la base de datos (definiciones, tablas, índices, y los propios datos), son guardados como un sólo fichero estándar en la máquina host. Este diseño simple se logra bloqueando todo el fichero de base de datos al principio de cada transacción.

En su versión 3, SQLite permite bases de datos de hasta 2 Terabytes de tamaño, y también permite la inclusión de campos tipo BLOB (almacenar largos arrays de bytes en un solo campo).

## 4. Android CyanogenMod

CyanogenMod es un firmware no oficial disponible para más de ochenta teléfonos móviles y tablets basados en el sistema operativo de código abierto Android. Está diseñado para aumentar el rendimiento y la fiabilidad el producto original y de compañías como Google, T-Mobile, HTC, etc. Ofrece características y mejoras que no se encuentran en las versiones oficiales de Android suministradas por los fabricantes, incluyendo, entre otras mejoras:

- Soporte para Free Lossless Audio Codec (FLAC)
- Multi-touch
- Caché comprimida (compcache).
- Una larga lista de APNs.
- Menú de reinicio
- Soporte para tethering mediante Wi-Fi, Bluetooth o USB.

Poco después de la introducción del teléfono HTC Dream en septiembre de 2008, la comunidad de desarrolladores Android encontró un método para obtener permisos de superusuario en el subsistema Linux de Android. Este descubrimiento, combinado con la naturaleza de código abierto de Android, permitió modificar los firmwares originales y reinstalarlos en el teléfono a voluntad.

La última versión de CyanogenMod se basa en Android 4.4.X (Jelly Bean). Las porciones de código modificado están escritas fundamentalmente por Cyanogen (Steve Kondik), pero

incluye contribuciones procedentes de la comunidad de desarrolladores xda-developers y de otros contribuyentes al proyecto.

En la versión 9.1 (correspondiente a Android 4.0 – Ice Cream Sandwich), fue añadida la emulación de tags únicamente con el protocolo ISO 14443-4.

Cyanogen también mantiene la recuperación de imagen utilizada en combinación con CyanogenMod. Proporciona un modo de arranque especial que se utiliza para crear copias de seguridad y restaurar el software del dispositivo, o reparar y actualizar el firmware.

## 5. Google App Engine

Google App Engine (GAE) es un servicio de alojamiento web que presta Google de forma gratuita hasta determinadas cuotas, el cual te permite ejecutar aplicaciones web sobre la infraestructura de Google. Las aplicaciones App Engine son fáciles de crear, de mantener y de ampliar al ir aumentando el tráfico y las necesidades de almacenamiento de datos. También permite limitar el acceso a determinados usuarios.

Las aplicaciones se ejecutan en un entorno seguro, lo que permite a App Engine distribuir peticiones a través de múltiples servidores y la ampliación de estos para satisfacer las demandas de tráfico. Cada aplicación se ejecuta dentro de su propio entorno seguro y confiable que es independiente del hardware, sistema operativo, o la ubicación física del servidor. [2]

Actualmente las aplicaciones GAE se implementan mediante los lenguajes de programación Python, Java, Go y PHP.

# CAPÍTULO 3: DESARROLLO TÉCNICO DEL PFC

---



Este capítulo recoge las partes concernientes al análisis, diseño y programación del sistema representadas con la mayor claridad y simplicidad posibles.

## 1. Análisis

### 1.1. Requisitos de usuario

En este apartado se detallan los requisitos que se han identificado en la fase de análisis del trabajo. Cada uno de los requisitos viene acompañado de ciertos datos compactados en una tabla con el siguiente formato:

<b>Identificador</b>	RUY-XX		
<b>Nombre</b>	Nombre de requisito		
<b>Descripción</b>	Descripción de requisito		
<b>Necesidad</b>	Necesidad de requisito	<b>Prioridad</b>	Prioridad de requisito
<b>Estabilidad</b>	Estabilidad de requisito	<b>Verificabilidad</b>	Verificabilidad de requisito

**Tabla 13:** Formato tabla de requisito de usuario

Cuyos campos significan:

- **Identificador:** identificador de requisito con la estructura RUY-XX, siendo:
  - **Y:**
    - **C:** requisito de usuario de capacidad.
    - **R:** requisito de usuario de restricción.
  - **XX:** número que identifica al requisito.
- **Nombre:** identificativo del requisito, es un pequeño resumen de lo que representa el requisito.
- **Descripción:** corresponde a la descripción del requisito.
- **Necesidad:** corresponde a lo imprescindible que resulta para el proyecto que dicho requisito sea implementado en el sistema. Los posibles valores son:
  - **Esencial:** es imprescindible que se implemente dicho requisito.
  - **Deseable:** se debe implementar el requisito pero no es algo esencial.
  - **Opcional:** se puede o no implementar el requisito ya que no es esencial para el correcto funcionamiento del sistema.
- **Prioridad:** indica la importancia del requisito en el proceso de diseño e implementación. Los posibles valores son:
  - **Alta:** es la prioridad máxima. El requisito debe ser diseñado y añadido al sistema en primer lugar.

- **Media:** el requisito debe ser diseñado y añadido al sistema tras haber acabado con los requisitos de prioridad alta.
- **Baja:** el requisito no es una gran prioridad para el proyecto, por lo que su realización se pospondrá para cuando se hayan realizado el resto de requisitos de mayor prioridad.
- **Estabilidad:** variabilidad del requisito ante posibles modificaciones en el transcurso del proyecto. Los posibles valores son:
  - **Estable:** el requisito tiene escasas posibilidades de que se modifique.
  - **No estable:** el requisito tendrá una alta posibilidad de que se modifique o incluso que se pueda eliminar del proyecto.
- **Verificabilidad:** nivel de complejidad para comprobar que el requisito se ha incluido en la implementación del sistema. Los posibles valores son:
  - **Alta:** la comprobación del requisito es complicada.
  - **Media:** el requisito se puede comprobar en un tiempo razonable y de manera fácil.
  - **Baja:** el requisito se comprueba de una manera rápida y sencilla.

#### 1.1.1. Requisitos de capacidad

Los requisitos de usuario de capacidad describen las capacidades que va a poseer la aplicación para resolver un problema o cumplir con un objetivo. A continuación se muestran los relativos a este proyecto:

<b>Identificador</b>	RUC-01		
<b>Nombre</b>	Lectura de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá leer tarjetas RFID de tipo Mifare Ultralight y Mifare Classic.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 14:** Requisito RUC-01 – Lectura de tarjetas RFID

<b>Identificador</b>	RUC-02		
<b>Nombre</b>	Selección de claves en lectura		
<b>Descripción</b>	La aplicación permitirá seleccionar las claves deseadas para leer tarjetas RFID.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 15:** Requisito RUC-02 – Selección de claves en lectura

<b>Identificador</b>	RUC-03		
<b>Nombre</b>	Escritura de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá escribir información en tarjetas RFID de tipo Mifare Ultralight y Mifare Classic.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 16: Requisito RUC-03 – Escritura de tarjetas RFID**

<b>Identificador</b>	RUC-04		
<b>Nombre</b>	Selección de claves en escritura		
<b>Descripción</b>	La aplicación permitirá seleccionar las claves deseadas para escribir tarjetas RFID.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 17: Requisito RUC-04 – Selección de claves en escritura**

<b>Identificador</b>	RUC-05		
<b>Nombre</b>	Gestión de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá la modificación y borrado de tarjetas RFID previamente leídas y almacenadas, así como la creación de nuevas tarjetas.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 18: Requisito RUC-05 – Gestión de tarjetas RFID**

<b>Identificador</b>	RUC-06		
<b>Nombre</b>	Visualización de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá ver el contenido de tarjetas RFID previamente leídas o almacenadas en formato ASCII, hexadecimal y como tarjeta de transporte.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 19: Requisito RUC-06 – Visualización de tarjetas RFID**

<b>Identificador</b>	RUC-07		
<b>Nombre</b>	Visualización de condiciones de acceso		
<b>Descripción</b>	La aplicación permitirá ver las condiciones de acceso de tarjetas RFID previamente leídas o almacenadas.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 20: Requisito RUC-07 – Visualización de condiciones de acceso**

<b>Identificador</b>	RUC-08		
<b>Nombre</b>	Importación de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá importar tarjetas RFID desde ficheros ubicados en el dispositivo.		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

**Tabla 21: Requisito RUC-08 – Importación de tarjetas RFID**

<b>Identificador</b>	RUC-09		
<b>Nombre</b>	Estadísticas		
<b>Descripción</b>	La aplicación realizará unas estadísticas de uso sobre las claves utilizadas para leer tarjetas Mifare Classic y las mandará a un backend.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 22: Requisito RUC-09 – Estadísticas

<b>Identificador</b>	RUC-10		
<b>Nombre</b>	Gestión de claves		
<b>Descripción</b>	La aplicación permitirá la creación, modificación y borrado de claves.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 23: Requisito RUC-10 – Gestión de claves

<b>Identificador</b>	RUC-11		
<b>Nombre</b>	Gestión de grupos de claves		
<b>Descripción</b>	La aplicación permitirá la creación, modificación y borrado de grupos de claves.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 24: Requisito RUC-11 – Gestión de grupos de claves

<b>Identificador</b>	RUC-12		
<b>Nombre</b>	Importación de claves		
<b>Descripción</b>	La aplicación permitirá importar claves desde ficheros ubicados en el dispositivo.		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

Tabla 25: Requisito RUC-12 – Importación de claves

<b>Identificador</b>	RUC-13		
<b>Nombre</b>	Activar tecnología NFC		
<b>Descripción</b>	La aplicación permitirá activar la tecnología NFC del dispositivo.		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

Tabla 26: Requisito RUC-13 – Activar tecnología NFC

### 1.1.2. Requisitos de restricción

Los requisitos de usuario de restricción definen las restricciones sobre la forma con la que se resuelve un problema o se logra un objetivo. A continuación se muestran los relativos a este proyecto:

<b>Identificador</b>	RUR-01		
<b>Nombre</b>	Lectura completa		
<b>Descripción</b>	La lectura de una tarjeta RFID debe ser completa, es decir, no pueden leerse unos bloques específicos.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 27: Requisito RUR-01 – Lectura completa

<b>Identificador</b>	RUR-02		
<b>Nombre</b>	Claves para lectura		
<b>Descripción</b>	Deben conocerse todas las claves para poder leer una tarjeta RFID de tipo Mifare Classic.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 28: Requisito RUR-02 – Claves para lectura

<b>Identificador</b>	RUR-03		
<b>Nombre</b>	Escritura completa		
<b>Descripción</b>	La escritura de una tarjeta RFID debe ser completa, es decir, no pueden escribirse unos bloques específicos.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 29: Requisito RUR-03 – Escritura completa

<b>Identificador</b>	RUR-04		
<b>Nombre</b>	Claves para escritura		
<b>Descripción</b>	Deben conocerse todas las claves para poder escribir en una tarjeta RFID de tipo Mifare Classic.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 30: Requisito RUR-04 – Claves para escritura

<b>Identificador</b>	RUR-05		
<b>Nombre</b>	Cancelación de escritura		
<b>Descripción</b>	La escritura de una tarjeta RFID no puede ser cancelada una vez que haya comenzado por riesgo de inutilizar la tarjeta.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 31: Requisito RUR-05 – Cancelación de escritura

<b>Identificador</b>	RUR-06		
<b>Nombre</b>	Tipo de tarjeta en escritura		
<b>Descripción</b>	El contenido de un tipo de tarjeta almacenado en el dispositivo solo puede ser escrito en una tarjeta del mismo tipo.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 32: Requisito RUR-06 – Tipo de tarjeta en escritura

<b>Identificador</b>	RUR-07		
<b>Nombre</b>	Nombre de tarjeta único		
<b>Descripción</b>	No pueden almacenarse dos tarjetas con el mismo nombre.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 33: Requisito RUR-07 – Nombre de tarjeta único

<b>Identificador</b>	RUR-08		
<b>Nombre</b>	Clave única		
<b>Descripción</b>	No pueden almacenarse dos claves iguales.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

Tabla 34: Requisito RUR-08 – Clave única

<b>Identificador</b>	RUR-09		
<b>Nombre</b>	Nombre de grupo de claves único		
<b>Descripción</b>	No pueden almacenarse dos grupos de claves con el mismo nombre.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

Tabla 35: Requisito RUR-09 – Nombre de grupo de claves único

<b>Identificador</b>	RUR-10		
<b>Nombre</b>	Nombre del tipo de tarjeta único		
<b>Descripción</b>	No pueden almacenarse dos tipos de tarjetas con el mismo nombre.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

Tabla 36: Requisito RUR-10 – Nombre del tipo de tarjeta único

<b>Identificador</b>	RUR-11		
<b>Nombre</b>	Formato tarjeta Mifare Ultralight		
<b>Descripción</b>	El formato de la tarjeta RFID de tipo Mifare Ultralight será de 16 páginas con 8 caracteres hexadecimales en cada uno de ellos.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 37: Requisito RUR-11 – Formato tarjeta Mifare Ultralight

<b>Identificador</b>	RUR-12		
<b>Nombre</b>	Formato tarjeta Mifare Classic Mini		
<b>Descripción</b>	El formato de la tarjeta RFID de tipo Mifare Classic Mini será de 5 sectores cada uno compuesto de 4 bloques de 32 caracteres hexadecimales.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 38: Requisito RUR-12 – Formato tarjeta Mifare Classic Mini

<b>Identificador</b>	RUR-13		
<b>Nombre</b>	Formato tarjeta Mifare Classic 1K		
<b>Descripción</b>	El formato de la tarjeta RFID de tipo Mifare Classic 1K será de 16 sectores cada uno compuesto de 4 bloques de 32 caracteres hexadecimales.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 39: Requisito RUR-13 – Formato tarjeta Mifare Classic 1K

<b>Identificador</b>	RUR-14		
<b>Nombre</b>	Formato tarjeta Mifare Classic 4K		
<b>Descripción</b>	El formato de la tarjeta RFID de tipo Mifare Classic 4K será de 40 sectores donde los 32 primeros estarán compuestos de 4 bloques y los 8 últimos de 16 bloques. En ambos casos cada bloque estará formado por 32 caracteres hexadecimales.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 40: Requisito RUR-14 – Formato tarjeta Mifare Classic 4K

<b>Identificador</b>	RUR-15		
<b>Nombre</b>	Formato clave		
<b>Descripción</b>	Las claves solo pueden contener valores hexadecimales.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

Tabla 41: Requisito RUR-15 – Formato clave

<b>Identificador</b>	RUR-16		
<b>Nombre</b>	Longitud clave		
<b>Descripción</b>	Las claves deben contener 12 caracteres alfanuméricos.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

Tabla 42: Requisito RUR-16 – Longitud clave

<b>Identificador</b>	RUR-17		
<b>Nombre</b>	Tarjeta por tipo		
<b>Descripción</b>	Una tarjeta solo puede relacionarse con un tipo de tarjeta.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 43: Requisito RUR-17 – Tarjeta por tipo

<b>Identificador</b>	RUR-18		
<b>Nombre</b>	Clave por tarjeta		
<b>Descripción</b>	Una clave puede relacionarse con múltiples tarjetas.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 44: Requisito RUR-18 – Clave por tarjeta

<b>Identificador</b>	RUR-19		
<b>Nombre</b>	Clave por grupo de clave		
<b>Descripción</b>	Una clave puede relacionarse con múltiples grupos de claves.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 45: Requisito RUR-19 – Clave por grupo de clave

<b>Identificador</b>	RUR-20		
<b>Nombre</b>	Claves por defecto		
<b>Descripción</b>	Por defecto la aplicación constará de unas claves que no podrán ser modificadas ni eliminadas.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Media
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

Tabla 46: Requisito RUR-20 – Claves por defecto

<b>Identificador</b>	RUR-21		
<b>Nombre</b>	Tipos de tarjeta por defecto		
<b>Descripción</b>	Por defecto la aplicación constará de los tipos de tarjetas “Control de acceso”, “Pasaporte” y “Transporte”.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Media
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

Tabla 47: Requisito RUR-21 – Tipos de tarjeta por defecto

<b>Identificador</b>	RUR-22		
<b>Nombre</b>	Ruta inicial en importe de tarjetas		
<b>Descripción</b>	Hasta que es modificada, la ruta para la importación de tarjetas es “/tags”.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Media
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

Tabla 48: Requisito RUR-22 – Ruta inicial en importe de tarjetas

<b>Identificador</b>	RUR-23		
<b>Nombre</b>	Ruta inicial en importe de claves		
<b>Descripción</b>	Hasta que es modificada, la ruta para la importación de claves es “/keys”.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Media
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

Tabla 49: Requisito RUR-23 – Ruta inicial en importe de claves

<b>Identificador</b>	RUR-24		
<b>Nombre</b>	Base de datos		
<b>Descripción</b>	Se dispone de una base de datos para almacenar los datos de su aplicación.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 50: Requisito RUR-24 – Base de datos



<b>Identificador</b>	RUR-25		
<b>Nombre</b>	Backend		
<b>Descripción</b>	Se dispone de un backend en un servidor remoto para almacenar la información de las estadísticas de uso de las claves.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 51: Requisito RUR-25 – Backend

<b>Identificador</b>	RUR-26		
<b>Nombre</b>	Lenguaje Android		
<b>Descripción</b>	Lenguaje Android (versión mínima Ice Cream Sandwich – 4.0.4) para el desarrollo de la aplicación.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 52: Requisito RUR-26 – Lenguaje Android

<b>Identificador</b>	RUR-27		
<b>Nombre</b>	Lenguaje Java		
<b>Descripción</b>	Lenguaje Java (v6) para el desarrollo del backend.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 53: Requisito RUR-27 – Lenguaje Java

<b>Identificador</b>	RUR-28		
<b>Nombre</b>	Lenguaje SQLite		
<b>Descripción</b>	Lenguaje SQLite para el desarrollo de la base de datos de la aplicación.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 54: Requisito RUR-28 – Lenguaje SQLite

<b>Identificador</b>	RUR-29		
<b>Nombre</b>	Compatibilidad Android		
<b>Descripción</b>	La aplicación será compatible con cualquier dispositivo con la versión de Android Jelly Bean (v4.1) o superior.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 55: Requisito RUR-29 – Compatibilidad Android

<b>Identificador</b>	RUR-30		
<b>Nombre</b>	Acceso concurrente al backend		
<b>Descripción</b>	Se permitirá el acceso concurrente a los datos ubicados en el backend permitiendo la modificación de información desde más de un dispositivo.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 56: Requisito RUR-30 – Acceso concurrente al backend

<b>Identificador</b>	RUR-31		
<b>Nombre</b>	Permisos de la aplicación		
<b>Descripción</b>	La aplicación tendrá los permisos necesarios para utilizar la tecnología NFC, lectura en tarjeta de almacenamiento externa, internet, y acceso al backend.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 57: Requisito RUR-31 – Permisos de la aplicación

<b>Identificador</b>	RUR-32		
<b>Nombre</b>	Idioma		
<b>Descripción</b>	La aplicación estará disponible en inglés y español.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 58: Requisito RUR-32 – Idioma

<b>Identificador</b>	RUR-33		
<b>Nombre</b>	Conexión a backend		
<b>Descripción</b>	La aplicación usará conexiones 3G o Wifi para comunicar el dispositivo con el backend.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 59: Requisito RUR-33 – Conexión a backend

<b>Identificador</b>	RUR-34		
<b>Nombre</b>	Tecnología NFC		
<b>Descripción</b>	La aplicación usará la tecnología NFC para la lectura y escritura de tarjetas RFID.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 60: Requisito RUR-34 – Tecnología NFC

<b>Identificador</b>	RUR-35		
<b>Nombre</b>	Aplicación eficiente		
<b>Descripción</b>	La aplicación debe ser rápida, eficaz e intuitiva.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 61: Requisito RUR-35 – Aplicación eficiente

<b>Identificador</b>	RUR-36		
<b>Nombre</b>	Aplicación escalable		
<b>Descripción</b>	La aplicación debe ser escalable ya que en un futuro pueden añadirse nuevas funcionalidades.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 62: Requisito RUR-36 – Aplicación escalable

<b>Identificador</b>	RUR-37		
<b>Nombre</b>	Gestión de fallos		
<b>Descripción</b>	La aplicación debe gestionar fallos.		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 63: Requisito RUR-37 – Gestión de fallos

### 1.1. Casos de uso

En este apartado se presenta el diagrama de casos de uso, una representación del comportamiento real del sistema y de cómo el usuario interactúa con él.

Primero se mostrará el diagrama de casos de uso en lenguaje gráfico Unified Modeling Language (UML) y a continuación se realizará una descripción textual de cada uno de estos casos.

Para la descripción textual se utiliza una tabla con el siguiente formato:

<b>Identificador</b>	CU-XX
<b>Nombre</b>	Nombre de caso de uso
<b>Actores</b>	Actores de caso de uso
<b>Objetivo</b>	Objetivo de caso de uso
<b>Precondiciones</b>	Precondiciones de caso de uso
<b>Postcondiciones</b>	Postcondiciones de caso de uso
<b>Escenario básico</b>	Escenario básico de caso de uso
<b>Escenario alternativo</b>	XX
<b>Descripción</b>	Descripción escenario alternativo
<b>Flujo alternativo</b>	Flujo de ejecución del escenario alternativo

Tabla 64: Formato tabla de caso de uso

Cuyos campos significan:

- **Identificador:** identificador de caso de uso con la estructura CU-XX, siendo XX el número que identifica al caso de uso.
- **Nombre:** se corresponde con el nombre asignado al caso de uso.
- **Actores:** es el rol o roles que encontraremos en el sistema. Es cualquier entidad externa al sistema que está relacionada con este y que le demanda una funcionalidad.
- **Objetivo:** estado que se quiere alcanzar tras finalizar el caso de uso.
- **Precondiciones:** estado del sistema antes de la ejecución del caso de uso.
- **Postcondiciones:** estado del sistema después de la ejecución del caso de uso.
- **Escenario básico:** secuencia de acciones de lo que tiene que hacer el caso de uso.

- **Escenario alternativo:** escenario a realizar cuando se produce algún inconveniente durante la ejecución del escenario básico. Este campo contiene el identificador del escenario alternativo con la estructura XX, siendo XX el número que lo identifica.
- **Descripción:** motivo por el que se produce el escenario alternativo.
- **Flujo alternativo:** secuencia de pasos detallados que se realiza en el escenario alternativo.

### 1.1.1. Diagrama de casos de uso

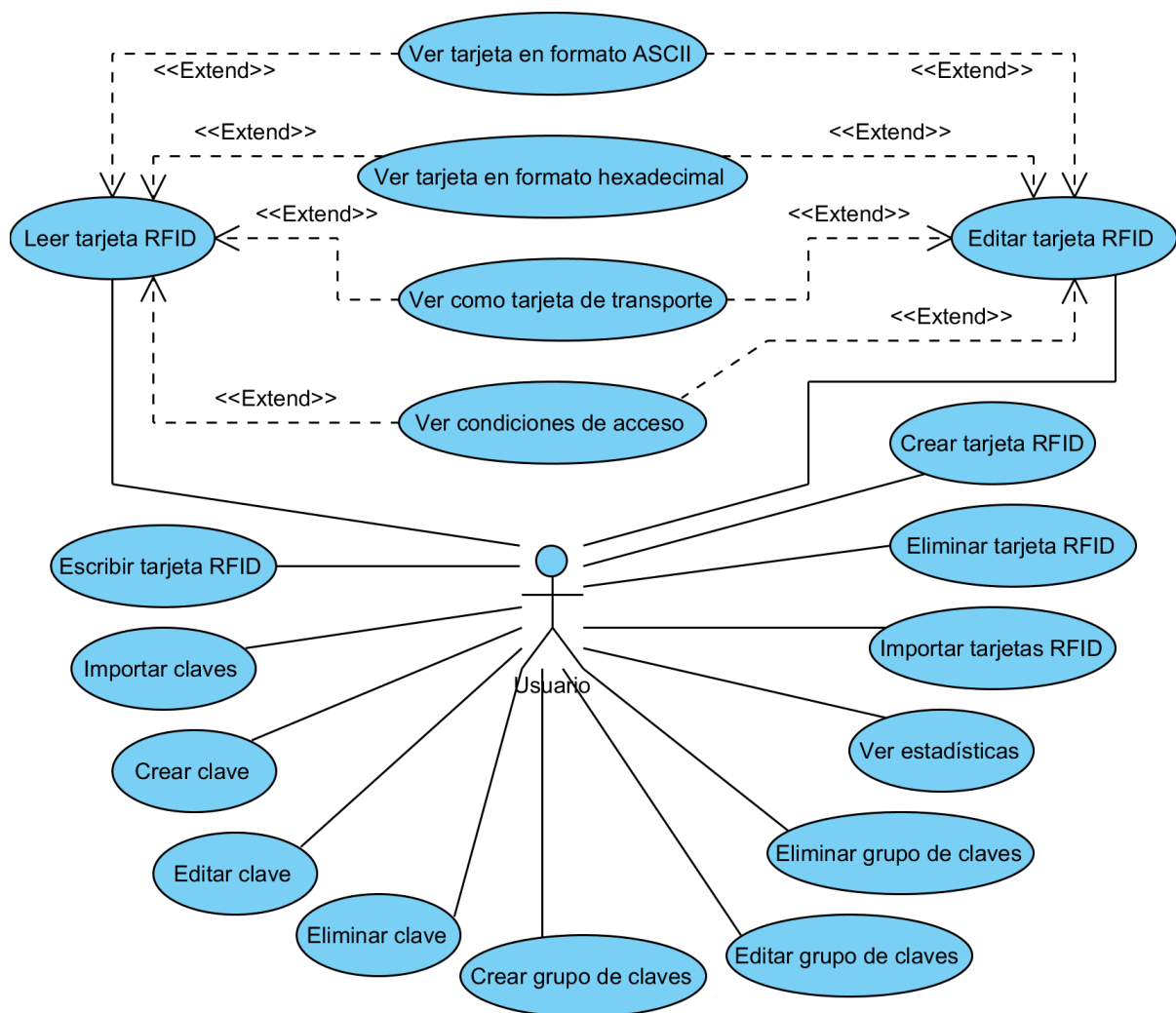


Ilustración 15: Casos de uso

### 1.1.2. Especificación detallada de los casos de uso

<b>Identificador</b>	CU-01
<b>Nombre</b>	Leer tarjeta RFID
<b>Actores</b>	Usuario
<b>Objetivo</b>	Leer el contenido de la tarjeta RFID y guardarlo en el dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>• Tener activada la tecnología NFC en el dispositivo.</li> <li>• Tener claves almacenadas en el dispositivo.</li> <li>• Tener grupos de claves almacenados en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>• El dispositivo mostrará por pantalla el mensaje temporal “Tag almacenado”.</li> <li>• La tarjeta RFID es mostrada por pantalla.</li> <li>• La tarjeta RFID es almacenada en la base de datos de la aplicación.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>1. Pulsar sobre el botón “Leer”.</li> <li>2. Seleccionar las claves utilizadas para autenticar y leer la tarjeta RFID (Ninguna, Todas o Grupos de claves).</li> <li>3. Acercar tarjeta RFID al teléfono.</li> <li>4. Escribir el nombre que identificará a esta tarjeta.</li> <li>5. Seleccionar el tipo de tarjeta.</li> <li>6. Modificar el contenido de la tarjeta que se considere estimado.</li> <li>7. Pulsar en el icono “Guardar” ubicado en la barra de menú.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	La información a guardar es incompleta o el formato del contenido de la tarjeta no es válido. La aplicación muestra el mensaje “Debe seleccionar el tipo de tarjeta”, “Debe escribir el nombre de la tarjeta”, “Algún sector no tiene 4 o 16 bloques”, “Algún bloque contiene datos no hexadecimal” o “Algún bloque no tiene 16 bytes (32 caracteres)”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>1. Corregir información errónea.</li> <li>2. Pulsar en el icono “Guardar” ubicado en la barra de menú.</li> </ol>
<b>Escenario alternativo</b>	02
<b>Descripción</b>	Ya existe una tarjeta RFID con el mismo nombre. La aplicación muestra un diálogo para reemplazar la tarjeta existente.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>1. Pulsar sobre el botón “Reemplazar”.</li> </ol>
<b>Escenario alternativo</b>	03
<b>Descripción</b>	Ya existe una tarjeta RFID con el mismo nombre. La aplicación muestra un diálogo para renombrar la nueva tarjeta.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>1. Pulsar sobre el botón “Renombrar”.</li> <li>2. Escribir el nuevo nombre de la tarjeta.</li> <li>3. Pulsar el botón “Aceptar”.</li> </ol>

Tabla 65: Caso de Uso CU-01 – Leer tarjeta RFID

<b>Identificador</b>	CU-02
<b>Nombre</b>	Escribir tarjeta RFID
<b>Actores</b>	Usuario
<b>Objetivo</b>	Escribir el contenido de una tarjeta RFID almacenada en el dispositivo en una tarjeta RFID externa.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>• Tener activada la tecnología NFC en el dispositivo.</li> <li>• Tener claves almacenadas en el dispositivo.</li> <li>• Tener grupos de claves almacenados en el dispositivo.</li> <li>• Tener almacenada al menos una tarjeta RFID en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>• La tarjeta RFID contendrá la información escrita por el dispositivo.</li> <li>• El dispositivo mostrará por pantalla la lista de tarjetas RFID almacenadas en el dispositivo.</li> <li>• El dispositivo mostrará por pantalla el mensaje temporal “Tag escrito”.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>1. Pulsar sobre el botón “Escribir”.</li> <li>2. Seleccionar la tarjeta que se quiere escribir.</li> <li>3. Seleccionar las claves utilizadas para autenticar y escribir la tarjeta RFID (Ninguna, Todas o Grupos de claves).</li> <li>4. Acercar tarjeta RFID al teléfono.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	La tarjeta externa contiene bloques que no pueden ser escritos. La aplicación muestra un diálogo con los sectores imposibles de escribir.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>1. Pulsar sobre el botón “Escribir tanto como sea posible”.</li> </ol>

Tabla 66: Caso de Uso CU-02 – Escribir Tarjeta RFID

<b>Identificador</b>	CU-03
<b>Nombre</b>	Editar tarjeta RFID
<b>Actores</b>	Usuario
<b>Objetivo</b>	Modificar el contenido de una tarjeta RFID almacenado en el dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Tener almacenada en el dispositivo aquella tarjeta RFID que va a ser modificada.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenada la tarjeta RFID ya modificada en su base de datos.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de tarjetas RFID almacenadas en el dispositivo.</li> <li>El dispositivo mostrará por pantalla el mensaje temporal “Tag almacenado”.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Ver escaneados”.</li> <li>Pulsar sobre la tarjeta RFID que se quiere modificar.</li> <li>Editar los datos que se consideren estimados.</li> <li>Pulsar en el icono “Guardar” ubicado en la barra de menú.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	La información a guardar es incompleta o el formato del contenido de la tarjeta no es válido. La aplicación muestra el mensaje “Debe seleccionar el tipo de tarjeta”, “Debe escribir el nombre de la tarjeta”, “Algún sector no tiene 4 o 16 bloques”, “Algún bloque contiene datos no hexadecimal” o “Algún bloque no tiene 16 bytes (32 caracteres)”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar en el icono “Guardar” ubicado en la barra de menú.</li> </ol>
<b>Escenario alternativo</b>	02
<b>Descripción</b>	Ya existe una tarjeta RFID con el mismo nombre. La aplicación muestra un diálogo para reemplazar la tarjeta existente.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Reemplazar”.</li> </ol>
<b>Escenario alternativo</b>	03
<b>Descripción</b>	Ya existe una tarjeta RFID con el mismo nombre. La aplicación muestra un diálogo para renombrar la nueva tarjeta.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Renombrar”.</li> <li>Escribir el nuevo nombre de la tarjeta.</li> <li>Pulsar el botón “Aceptar”.</li> </ol>

**Tabla 67:** Caso de Uso CU-03 – Editar tarjeta RFID

<b>Identificador</b>	CU-04
<b>Nombre</b>	Crear tarjeta RFID
<b>Actores</b>	Usuario
<b>Objetivo</b>	Crear y almacenar el contenido de una tarjeta RFID en la base de datos del dispositivo.
<b>Precondiciones</b>	
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenada la nueva tarjeta RFID en su base de datos.</li> <li>El dispositivo mostrará por pantalla el mensaje “Tag almacenado”.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de tarjetas RFID almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Ver escaneados”.</li> <li>Seleccionar la opción “Crear tag” en el menú desplegable.</li> <li>Seleccionar el tamaño de la tarjeta a crear (Mifare Ultralight, Mifare Classic Mini, Mifare Classic 1K o Mifare Classic 4K).</li> <li>Escribir el nombre que identificará a esta tarjeta.</li> <li>Seleccionar el tipo de tarjeta.</li> <li>Modificar el contenido de la tarjeta que se considere estimado.</li> <li>Pulsar en el icono “Guardar” ubicado en la barra de menú.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	La información a guardar es incompleta o el formato del contenido de la tarjeta no es válido. La aplicación muestra el mensaje “Debe seleccionar el tipo de tarjeta”, “Debe escribir el nombre de la tarjeta”, “Algún sector no tiene 4 o 16 bloques”, “Algún bloque contiene datos no hexadecimal” o “Algún bloque no tiene 16 bytes (32 caracteres)”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar en el icono “Guardar” ubicado en la barra de menú.</li> </ol>
<b>Escenario alternativo</b>	02
<b>Descripción</b>	Ya existe una tarjeta RFID con el mismo nombre. La aplicación muestra un diálogo para reemplazar la tarjeta existente.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Reemplazar”.</li> </ol>
<b>Escenario alternativo</b>	03
<b>Descripción</b>	Ya existe una tarjeta RFID con el mismo nombre. La aplicación muestra un diálogo para renombrar la nueva tarjeta.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Renombrar”.</li> <li>Escribir el nuevo nombre de la tarjeta.</li> <li>Pulsar el botón “Aceptar”.</li> </ol>

**Tabla 68:** Caso de Uso CU-04 – Crear tarjeta RFID



<b>Identificador</b>	CU-05
<b>Nombre</b>	Eliminar tarjeta RFID
<b>Actores</b>	Usuario
<b>Objetivo</b>	Eliminar una tarjeta RFID de la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Tener almacenada en el dispositivo aquella tarjeta RFID que va a ser eliminada.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>La tarjeta RFID no estará almacenada en el dispositivo.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de tarjetas RFID almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Ver escaneados”.</li> <li>Mantener pulsada la tarjeta RFID de la lista a eliminar.</li> <li>Pulsar en el botón “Aceptar”.</li> </ol>

**Tabla 69:** Caso de Uso CU-05 – Eliminar tarjeta RFID

<b>Identificador</b>	CU-06
<b>Nombre</b>	Importar tarjetas RFID
<b>Actores</b>	Usuario
<b>Objetivo</b>	Importar tarjetas RFID ubicadas en ficheros dentro del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Poseer tarjetas RFID almacenadas en ficheros con extensión .dmp dentro del dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenadas las nuevas tarjetas RFID en su base de datos.</li> <li>El dispositivo mostrará por pantalla el mensaje “Tags almacenados”.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de tarjetas RFID almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Ver escaneados”.</li> <li>Seleccionar la opción “Importar tags” en el menú desplegable.</li> <li>Escribir el directorio donde se encuentran las tarjetas RFID a importar.</li> <li>Activar/Desactivar “Importar claves de tarjeta” para almacenar las claves de las tarjetas RFID a importar.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

<b>Escenario alternativo</b>	01
<b>Descripción</b>	No se ha indicado ningún directorio del que importar tarjetas RFID. La aplicación muestra el mensaje “Ubicación del fichero de tags vacío”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Escribir el directorio donde se encuentran las tarjetas RFID a importar.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

<b>Escenario alternativo</b>	02
<b>Descripción</b>	El directorio indicado no existe. La aplicación muestra el mensaje “Archivo no encontrado”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Escribir el directorio correcto donde se encuentran las tarjetas RFID a importar.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

**Tabla 70:** Caso de Uso CU-06 – Importar tarjetas RFID

<b>Identificador</b>	CU-07
<b>Nombre</b>	Ver tarjeta en formato ASCII
<b>Actores</b>	Usuario
<b>Objetivo</b>	Ver el contenido de una tarjeta RFID en formato ASCII.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Haber leído o tener almacenada una tarjeta RFID en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo mostrará por pantalla el contenido de la tarjeta RFID con formato ASCII.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>El usuario lee [Caso de Uso CU-01 – Leer tarjeta RFID] o edita [Caso de Uso CU-03 – Editar tarjeta RFID] una tarjeta RFID.</li> <li>Seleccionar la opción “Ver como ASCII” en el menú desplegable.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	El formato del contenido de la tarjeta no es válido. La aplicación muestra el mensaje “Algún sector no tiene 4 o 16 bloques”, “Algún bloque contiene datos no hexadecimal” o “Algún bloque no tiene 16 bytes (32 caracteres)”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar sobre la opción “Ver como ASCII” en el menú desplegable.</li> </ol>

**Tabla 71: Caso de Uso CU-07 – Ver tarjeta en formato ASCII**

<b>Identificador</b>	CU-08
<b>Nombre</b>	Ver tarjeta en formato hexadecimal
<b>Actores</b>	Usuario
<b>Objetivo</b>	Ver el contenido de una tarjeta RFID en formato hexadecimal.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Haber leído o tener almacenada una tarjeta RFID en el dispositivo.</li> <li>Estar visualizando el contenido de la tarjeta en formato ASCII.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo mostrará por pantalla el contenido de la tarjeta RFID con formato hexadecimal.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>El usuario ve la tarjeta en formato ASCII [Caso de Uso CU-07 – Ver tarjeta en formato ASCII].</li> <li>Seleccionar la opción “Ver como HEX” en el menú desplegable.</li> </ol>

**Tabla 72: Caso de Uso CU-08 – Ver tarjeta en formato hexadecimal**

<b>Identificador</b>	CU-09
<b>Nombre</b>	Ver como tarjeta de transporte
<b>Actores</b>	Usuario
<b>Objetivo</b>	Ver el contenido de una tarjeta RFID como tarjeta de transporte.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Haber leído o tener almacenada una tarjeta RFID en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo mostrará por pantalla el contenido de la tarjeta RFID como tarjeta de transporte.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>El usuario lee [Caso de Uso CU-01 – Leer tarjeta RFID] o edita [Caso de Uso CU-03 – Editar tarjeta RFID] una tarjeta RFID.</li> <li>Seleccionar la opción “Ver como tarjeta de transporte” en el menú desplegable.</li> </ol>

<b>Escenario alternativo</b>	01
<b>Descripción</b>	El formato del contenido de la tarjeta no es válido. La aplicación muestra el mensaje “Algún sector no tiene 4 o 16 bloques”, “Algún bloque contiene datos no hexadecimal” o “Algún bloque no tiene 16 bytes (32 caracteres)”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar sobre la opción “Ver como tarjeta de transporte” en el menú desplegable.</li> </ol>

**Tabla 73: Caso de Uso CU-09 – Ver como tarjeta de transporte**

<b>Identificador</b>	CU-10
<b>Nombre</b>	Ver condiciones de acceso
<b>Actores</b>	Usuario
<b>Objetivo</b>	Ver las condiciones de acceso de una tarjeta RFID.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Haber leído o tener almacenada una tarjeta RFID en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo mostrara por pantalla las condiciones de acceso de la tarjeta RFID.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>El usuario lee [Caso de Uso CU-01 – Leer tarjeta RFID] o edita [Caso de Uso CU-03 – Editar tarjeta RFID] una tarjeta RFID.</li> <li>Seleccionar la opción “Ver condiciones de acceso” en el menú desplegable.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	El formato del contenido de la tarjeta no es válido. La aplicación muestra el mensaje “Algún sector no tiene 4 o 16 bloques”, “Algún bloque contiene datos no hexadecimal” o “Algún bloque no tiene 16 bytes (32 caracteres)”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar sobre la opción “Ver condiciones de acceso” en el menú desplegable.</li> </ol>

Tabla 74: Caso de Uso CU-10 – Ver condiciones de acceso

<b>Identificador</b>	CU-11
<b>Nombre</b>	Ver estadísticas
<b>Actores</b>	Usuario
<b>Objetivo</b>	Ver las estadísticas de uso de las claves empleadas para la lectura y escritura de tarjetas RFID.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo debe tener acceso a internet.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo mostrara por pantalla las estadísticas de las claves utilizadas o el mensaje “No existen claves” si no hay claves almacenadas en el servidor remoto.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Estadísticas”.</li> </ol>

Tabla 75: Caso de Uso CU-11 – Ver estadísticas

<b>Identificador</b>	CU-12
<b>Nombre</b>	Crear clave
<b>Actores</b>	Usuario
<b>Objetivo</b>	Almacenar una o varias claves nuevas en la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Las claves a crear no estén almacenadas en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenadas las nuevas claves en su base de datos.</li> <li>El dispositivo mostrará por pantalla el mensaje “Claves almacenadas”.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de claves almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Claves”.</li> <li>Pulsar en el icono “Nuevas claves” ubicado en la barra de menú.</li> <li>Escribir las claves separadas por un salto de línea.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	La clave escrita posee una longitud inválida. La aplicación muestra el mensaje “La clave debe tener 12 caracteres alfanuméricos”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

Tabla 76: Caso de Uso CU-12 – Crear clave

<b>Identificador</b>	CU-13
<b>Nombre</b>	Editar clave
<b>Actores</b>	Usuario
<b>Objetivo</b>	Editar una clave de la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>La clave a modificar ya debe estar almacenada en el dispositivo.</li> <li>La clave a modificar debe haber sido creada previamente por el usuario.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenada la nueva clave en su base de datos.</li> <li>El dispositivo mostrará por pantalla el mensaje “Clave modificada”.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de claves almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Claves”.</li> <li>Pulsar sobre la clave a modificar.</li> <li>Editar la clave.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	La clave escrita posee una longitud inválida. La aplicación muestra el mensaje “La clave debe tener 12 caracteres alfanuméricos”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Corregir información errónea.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

Tabla 77: Caso de Uso CU-13 – Editar clave

<b>Identificador</b>	CU-14
<b>Nombre</b>	Eliminar clave
<b>Actores</b>	Usuario
<b>Objetivo</b>	Eliminar una clave de la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>La clave a eliminar ya debe estar almacenada en el dispositivo.</li> <li>La clave a eliminar debe haber sido creada por el usuario.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>La clave no estará almacenada en la base de datos del dispositivo.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de claves almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Claves”.</li> <li>Mantener pulsada la clave a eliminar.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

**Tabla 78:** Caso de Uso CU-14 – Eliminar clave

<b>Identificador</b>	CU-15
<b>Nombre</b>	Crear grupo de claves
<b>Actores</b>	Usuario
<b>Objetivo</b>	Almacenar un grupo de claves en la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Las claves que formarán el grupo de claves deben estar previamente almacenadas en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenado el nuevo grupo de claves en su base de datos.</li> <li>El dispositivo mostrará por pantalla el mensaje “Grupo de claves almacenado”.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de los grupos de claves almacenados en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Claves”.</li> <li>Seleccionar la opción “Crear grupo de claves” en el menú desplegable.</li> <li>Escribir el nombre que identificará al grupo de claves.</li> <li>Seleccionar claves.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

<b>Escenario alternativo</b>	01
<b>Descripción</b>	El nombre del grupo de claves está vacío. La aplicación muestra el mensaje “El nombre del grupo debe tener contenido”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Escribir el nombre que identificará al grupo de claves.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

<b>Escenario alternativo</b>	02
<b>Descripción</b>	No se ha seleccionado ninguna clave de la lista. La aplicación muestra el mensaje “No hay claves seleccionadas”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Seleccionar claves.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

**Tabla 79:** Caso de Uso CU-15 – Crear grupo de claves

<b>Identificador</b>	CU-16
<b>Nombre</b>	Editar grupo de claves
<b>Actores</b>	Usuario
<b>Objetivo</b>	Modificar un grupo de claves de la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>Las claves que formarán el grupo de claves deben estar previamente almacenadas en el dispositivo.</li> <li>El grupo de claves a modificar debe estar previamente almacenado en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El dispositivo tendrá almacenado en su base de datos el grupo de claves modificado.</li> <li>El dispositivo mostrará por pantalla el mensaje “Grupo de claves modificado”.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de los grupos de claves almacenados en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Claves”.</li> <li>Arrastrar la pantalla hacia la derecha para cambiar a la sección “GRUPOS”.</li> <li>Seleccionar de la lista el grupo de claves a modificar.</li> <li>Pulsar en el icono “Editar” ubicado en la barra de menú.</li> <li>Modificar los datos que se deseen.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Escenario alternativo</b>	o1
<b>Descripción</b>	El nombre del grupo de claves está vacío. La aplicación muestra el mensaje “El nombre del grupo debe tener contenido”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Escribir el nombre que identificará al grupo de claves.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Escenario alternativo</b>	o2
<b>Descripción</b>	No se ha seleccionado ninguna clave de la lista. La aplicación muestra el mensaje “No hay claves seleccionadas”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>Seleccionar claves.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

Tabla 80: Caso de Uso CU-16 – Editar grupo de claves

<b>Identificador</b>	CU-17
<b>Nombre</b>	Eliminar grupo de claves
<b>Actores</b>	Usuario
<b>Objetivo</b>	Eliminar un grupo de claves de la base de datos del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>El grupo de claves debe estar almacenado en el dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>El grupo de claves no estará almacenada en la base de datos del dispositivo.</li> <li>El dispositivo mostrará por pantalla la lista actualizada de los grupos de claves almacenados en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>Pulsar sobre el botón “Claves”.</li> <li>Arrastrar la pantalla hacia la derecha para cambiar a la sección “GRUPOS”.</li> <li>Mantener pulsado en la lista el grupo de claves a eliminar.</li> <li>Pulsar sobre el botón “Aceptar”.</li> </ol>

Tabla 81: Caso de Uso CU-17 – Eliminar grupo de claves

<b>Identificador</b>	CU-18
<b>Nombre</b>	Importar claves
<b>Actores</b>	Usuario
<b>Objetivo</b>	Importar claves ubicadas en ficheros dentro del dispositivo.
<b>Precondiciones</b>	<ul style="list-style-type: none"> <li>• Poseer tarjetas RFID almacenadas en ficheros con extensión .dmp dentro del dispositivo.</li> </ul>
<b>Postcondiciones</b>	<ul style="list-style-type: none"> <li>• El dispositivo tendrá almacenadas las nuevas claves en su base de datos.</li> <li>• El dispositivo mostrará por pantalla el mensaje “Claves almacenadas”.</li> <li>• El dispositivo mostrará por pantalla la lista actualizada de claves almacenadas en el dispositivo.</li> </ul>
<b>Escenario básico</b>	<ol style="list-style-type: none"> <li>1. Pulsar sobre el botón “Claves”.</li> <li>2. Seleccionar la opción “Importar claves” en el menú desplegable.</li> <li>3. Escribir el directorio donde se encuentran los ficheros de claves a importar.</li> <li>4. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Escenario alternativo</b>	01
<b>Descripción</b>	No se ha indicado ningún directorio del que importar claves. La aplicación muestra el mensaje “Ubicación del fichero de claves vacío”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>1. Seleccionar la opción “Importar claves” en el menú desplegable.</li> <li>2. Escribir el directorio donde se encuentran los ficheros de claves a importar.</li> <li>3. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Escenario alternativo</b>	02
<b>Descripción</b>	El directorio indicado no existe. La aplicación muestra el mensaje “Archivo no encontrado”.
<b>Flujo alternativo</b>	<ol style="list-style-type: none"> <li>1. Seleccionar la opción “Importar claves” en el menú desplegable.</li> <li>2. Escribir el directorio correcto donde se encuentran los ficheros de claves a importar.</li> <li>3. Pulsar sobre el botón “Aceptar”.</li> </ol>

Tabla 82: Caso de Uso CU-18 – Importar claves

## 1.2. Requisitos software

En este apartado se detallan los requisitos software funcionales y no funcionales. Cada uno de los requisitos viene acompañado de ciertos datos compactados en una tabla con el siguiente formato:

<b>Identificador</b>	RSY-XX	<b>Tipo</b>	Tipo de requisito
<b>Nombre</b>	Nombre de requisito		
<b>Descripción</b>	Descripción de requisito		
<b>Fuente</b>	Origen de requisito		
<b>Necesidad</b>	Necesidad de requisito	<b>Prioridad</b>	Prioridad de requisito
<b>Estabilidad</b>	Estabilidad de requisito	<b>Verificabilidad</b>	Verificabilidad de requisito

Tabla 83: Formato tabla de requisito software

Cuyos campos significan:

- **Identificador:** identificador de requisito con la estructura RSY-XX, siendo:

- **Y:**
  - **F:** requisito software funcional.
  - **NF-OP:** requisito software no funcional de operación.
  - **NF-INT:** requisito software no funcional de interfaz.
  - **NF-REC:** requisito software no funcional de recursos.
  - **NF-REN:** requisito software no funcional de rendimiento.
- **XX:** número que identifica al requisito.
- **Tipo:** define el tipo de requerimiento. Solamente puede tomar los valores:
  - **Funcional:** describen las funcionalidades del sistema, es decir, lo que éste debe hacer.
  - **Operación:** identifican a los requisitos no funcionales de operación.
  - **Interfaz:** identifican a los requisitos no funcionales de interfaz.
  - **Recurso:** identifican a los requisitos no funcionales de recursos.
  - **Rendimiento:** identifican a los requisitos no funcionales de rendimiento.
- **Nombre:** identificativo del requisito, es un pequeño resumen de lo que representa el requisito.
- **Descripción:** corresponde a la descripción del requisito.
- **Fuente:** indica el origen de donde proviene el requisito. En el caso de los Requisitos Software dicha fuente hará referencia a uno o varios Requisitos de Usuario definidos en el apartado 1.1 Requisitos de usuario.
- **Necesidad:** corresponde a lo imprescindible que resulta para el proyecto que dicho requisito sea implementado en el sistema. Los posibles valores son:
  - **Esencial:** es imprescindible que se implemente dicho requisito.
  - **Deseable:** se debe implementar el requisito pero no es algo esencial.
  - **Opcional:** se puede o no implementar el requisito ya que no es esencial para el correcto funcionamiento del sistema.
- **Prioridad:** indica la importancia del requisito en el proceso de diseño e implementación. Los posibles valores son:
  - **Alta:** es la prioridad máxima. El requisito debe ser diseñado y añadido al sistema en primer lugar.
  - **Media:** el requisito debe ser diseñado y añadido al sistema tras haber acabado con los requisitos de prioridad alta.



- **Baja:** el requisito no es una gran prioridad para el proyecto, por lo que su realización se pospondrá para cuando se hayan realizado el resto de requisitos de mayor prioridad.
- **Estabilidad:** variabilidad del requisito ante posibles modificaciones en el transcurso del proyecto. Los posibles valores son:
  - **Estable:** el requisito tiene escasas posibilidades de que se modifique.
  - **No estable:** el requisito tendrá una alta posibilidad de que se modifique o incluso que se pueda eliminar del proyecto.
- **Verificabilidad:** nivel de complejidad para comprobar que el requisito se ha incluido en la implementación del sistema. Los posibles valores son:
  - **Alta:** la comprobación del requisito es complicada.
  - **Media:** el requisito se puede comprobar en un tiempo razonable y de manera fácil.
  - **Baja:** el requisito se comprueba de una manera rápida y sencilla.

### 1.2.1. Requisitos funcionales

Los requisitos software funcionales especifican los servicios y funcionalidades de la aplicación. A continuación se muestran los relativos a este proyecto:

<b>Identificador</b>	RSF-01	<b>Tipo</b>	Funcional
<b>Nombre</b>	Lectura tarjetas Mifare Ultralight		
<b>Descripción</b>	La aplicación permitirá la lectura de tarjetas RFID de tipo Mifare Ultralight. Para almacenar la tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-01, RUR-01, RUR-07, RUR-11, RUR-17, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 84: Requisito RSF-01 – Lectura tarjetas Mifare Ultralight

<b>Identificador</b>	RSF-02	<b>Tipo</b>	Funcional
<b>Nombre</b>	Lectura tarjetas Mifare Classic Mini		
<b>Descripción</b>	La aplicación permitirá la lectura de tarjetas RFID de tipo Mifare Classic Mini. Para almacenar la tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-01, RUR-01, RUR-02, RUR-07, RUR-12, RUR-17, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 85: Requisito RSF-02 – Lectura tarjetas Mifare Classic Mini

<b>Identificador</b>	RSF-03	<b>Tipo</b>	Funcional
<b>Nombre</b>	Lectura tarjetas Mifare Classic 1K		
<b>Descripción</b>	La aplicación permitirá la lectura de tarjetas RFID de tipo Mifare Classic 1K. Para almacenar la tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-01, RUR-01, RUR-02, RUR-07, RUR-13, RUR-17, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 86: Requisito RSF-03 – Lectura tarjetas Mifare Classic 1K

<b>Identificador</b>	RSF-04	<b>Tipo</b>	Funcional
<b>Nombre</b>	Lectura tarjetas Mifare Classic 4K		
<b>Descripción</b>	La aplicación permitirá la lectura de tarjetas RFID de tipo Mifare Classic 4K. Para almacenar la tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-01, RUR-01, RUR-02, RUR-07, RUR-14, RUR-17, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 87: Requisito RSF-04 – Lectura tarjetas Mifare Classic 4K

<b>Identificador</b>	RSF-05	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de tipos de tarjetas		
<b>Descripción</b>	La aplicación permitirá crear nuevos tipos de tarjetas RFID mientras se está leyendo, creando o modificando una tarjeta RFID.		
<b>Fuente</b>	RUC-01, RUR-10, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 88: Requisito RSF-05 – Creación de tipos de tarjetas

<b>Identificador</b>	RSF-06	<b>Tipo</b>	Funcional
<b>Nombre</b>	Renombrar tarjeta RFID		
<b>Descripción</b>	La aplicación permitirá renombrar una tarjeta RFID al intentar almacenarla con un nombre ya existente en la base de datos.		
<b>Fuente</b>	RUC-01, RUC-05		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 89: Requisito RSF-06 – Renombrar tarjeta RFID

<b>Identificador</b>	RSF-07	<b>Tipo</b>	Funcional
<b>Nombre</b>	Reemplazar tarjeta RFID		
<b>Descripción</b>	La aplicación permitirá reemplazar una tarjeta RFID por otra al intentar almacenarla con un nombre ya existente en la base de datos.		
<b>Fuente</b>	RUC-01, RUC-05		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 90: Requisito RSF-07 – Reemplazar tarjeta RFID

<b>Identificador</b>	RSF-o8	<b>Tipo</b>	Funcional
<b>Nombre</b>	Valor por defecto de bloque		
<b>Descripción</b>	El contenido de un bloque es rellenado con ‘-‘ cuando no puede ser leído a pesar de haber autenticado su sector correctamente.		
<b>Fuente</b>	RUC-01		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 91:** Requisito RSF-o8 – Valor por defecto de bloque

<b>Identificador</b>	RSF-09	<b>Tipo</b>	Funcional
<b>Nombre</b>	Todas las claves para leer tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá utilizar todas las claves para leer tarjetas RFID.		
<b>Fuente</b>	RUC-02, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 92:** Requisito RSF-09 – Todas las claves para leer tarjetas RFID

<b>Identificador</b>	RSF-10	<b>Tipo</b>	Funcional
<b>Nombre</b>	Grupos de claves para leer tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá seleccionar grupos de claves para leer tarjetas RFID.		
<b>Fuente</b>	RUC-02, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 93:** Requisito RSF-10 – Grupos de claves para leer tarjetas RFID

<b>Identificador</b>	RSF-11	<b>Tipo</b>	Funcional
<b>Nombre</b>	Ninguna clave para leer tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá no utilizar ninguna clave ni grupos de claves para leer tarjetas RFID.		
<b>Fuente</b>	RUC-02		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 94:** Requisito RSF-11 – Ninguna clave para leer tarjetas RFID

<b>Identificador</b>	RSF-12	<b>Tipo</b>	Funcional
<b>Nombre</b>	Escritura tarjetas Mifare Ultralight		
<b>Descripción</b>	La aplicación permitirá la escritura de tarjetas RFID de tipo Mifare Ultralight.		
<b>Fuente</b>	RUC-03, RUR-03, RUR-05, RUR-06, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 95:** Requisito RSF-12 – Escritura tarjetas Mifare Ultralight

<b>Identificador</b>	RSF-13	<b>Tipo</b>	Funcional
<b>Nombre</b>	Escritura tarjetas Mifare Classic Mini		
<b>Descripción</b>	La aplicación permitirá la escritura de tarjetas RFID de tipo Mifare Classic Mini.		
<b>Fuente</b>	RUC-03, RUR-03, RUR-04, RUR-05, RUR-06, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 96: Requisito RSF-13 – Escritura tarjetas Mifare Classic Mini

<b>Identificador</b>	RSF-14	<b>Tipo</b>	Funcional
<b>Nombre</b>	Escritura tarjetas Mifare Classic 1K		
<b>Descripción</b>	La aplicación permitirá la escritura de tarjetas RFID de tipo Mifare Classic 1K.		
<b>Fuente</b>	RUC-03, RUR-03, RUR-04, RUR-05, RUR-06, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 97: Requisito RSF-14 – Escritura tarjetas Mifare Classic 1K

<b>Identificador</b>	RSF-15	<b>Tipo</b>	Funcional
<b>Nombre</b>	Escritura tarjetas Mifare Classic 4K		
<b>Descripción</b>	La aplicación permitirá la escritura de tarjetas RFID de tipo Mifare Classic 4K.		
<b>Fuente</b>	RUC-03, RUR-03, RUR-04, RUR-05, RUR-06, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 98: Requisito RSF-15 – Escritura tarjetas Mifare Classic 4K

<b>Identificador</b>	RSF-16	<b>Tipo</b>	Funcional
<b>Nombre</b>	Todas las claves para escribir tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá seleccionar todas las claves para escribir tarjetas RFID.		
<b>Fuente</b>	RUC-04, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 99: Requisito RSF-16 – Todas las claves para escribir tarjetas RFID

<b>Identificador</b>	RSF-17	<b>Tipo</b>	Funcional
<b>Nombre</b>	Grupos de claves para escribir tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá seleccionar grupos de claves para escribir tarjetas RFID.		
<b>Fuente</b>	RUC-04, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 100: Requisito RSF-17 – Grupos de claves para escribir tarjetas RFID

<b>Identificador</b>	RSF-18	<b>Tipo</b>	Funcional
<b>Nombre</b>	Ninguna clave para escribir tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá no seleccionar ninguna clave ni grupos de claves para escribir tarjetas RFID.		
<b>Fuente</b>	RUC-04		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 101: Requisito RSF-18 – Ninguna clave para escribir tarjetas RFID

<b>Identificador</b>	RSF-19	<b>Tipo</b>	Funcional
<b>Nombre</b>	Claves en backend		
<b>Descripción</b>	Las claves utilizadas para la lectura y escritura de tarjetas RFID son almacenadas en el backend junto con el número total de veces que han sido utilizadas en ambos tipos de operaciones.		
<b>Fuente</b>	RUR-25, RUR-30, RUR-31, RUR-33		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 102:** Requisito RSF-19 – Claves en backend

<b>Identificador</b>	RSF-20	<b>Tipo</b>	Funcional
<b>Nombre</b>	Modificación de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá modificar tarjetas RFID previamente almacenadas. Para modificar una tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-05, RUR-07, RUR-11, RUR-12, RUR-13, RUR-14, RUR-17, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 103:** Requisito RSF-20 – Modificación de tarjetas RFID

<b>Identificador</b>	RSF-21	<b>Tipo</b>	Funcional
<b>Nombre</b>	Borrado de tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá borrar tarjetas RFID previamente almacenadas.		
<b>Fuente</b>	RUC-05, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 104:** Requisito RSF-21 – Borrado de tarjetas RFID

<b>Identificador</b>	RSF-22	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de tarjetas Mifare Ultralight		
<b>Descripción</b>	La aplicación permitirá crear tarjetas RFID de tipo Mifare Ultralight. Para modificar una tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-05, RUR-07, RUR-11, RUR-17, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 105:** Requisito RSF-22 – Creación de tarjetas Mifare Ultralight

<b>Identificador</b>	RSF-23	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de tarjetas Mifare Classic Mini		
<b>Descripción</b>	La aplicación permitirá crear tarjetas RFID de tipo Mifare Classic Mini. Para modificar una tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-05, RUR-07, RUR-12, RUR-17, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 106: Requisito RSF-23 – Creación de tarjetas Mifare Classic Mini**

<b>Identificador</b>	RSF-24	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de tarjetas Mifare Classic 1K		
<b>Descripción</b>	La aplicación permitirá crear tarjetas RFID de tipo Mifare Classic 1K. Para modificar una tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-05, RUR-07, RUR-13, RUR-17, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 107: Requisito RSF-24 – Creación de tarjetas Mifare Classic 1K**

<b>Identificador</b>	RSF-25	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de tarjetas Mifare Classic 4K		
<b>Descripción</b>	La aplicación permitirá crear tarjetas RFID de tipo Mifare Classic 4K. Para modificar una tarjeta el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de tarjeta</li> <li>• Tipo de tarjeta</li> <li>• Contenido de tarjeta</li> </ul>		
<b>Fuente</b>	RUC-05, RUR-07, RUR-14, RUR-17, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 108: Requisito RSF-25 – Creación de tarjetas Mifare Classic 4K**

<b>Identificador</b>	RSF-26	<b>Tipo</b>	Funcional
<b>Nombre</b>	Valores por defecto en nuevas tarjetas		
<b>Descripción</b>	Cuando una tarjeta es creada todo su contenido es rellenado con ceros.		
<b>Fuente</b>	RUC-05, RUR-11, RUR-12, RUR-13, RUR-14		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 109: Requisito RSF-26 – Valores por defecto en nuevas tarjetas**

<b>Identificador</b>	RSF-27	<b>Tipo</b>	Funcional
<b>Nombre</b>	Visualización en formato ASCII		
<b>Descripción</b>	La aplicación permitirá ver el contenido de tarjetas RFID previamente leídas o almacenadas en formato ASCII.		
<b>Fuente</b>	RUC-o6		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 110:** Requisito RSF-27 – Visualización en formato ASCII

<b>Identificador</b>	RSF-28	<b>Tipo</b>	Funcional
<b>Nombre</b>	Visualización en formato hexadecimal		
<b>Descripción</b>	La aplicación permitirá ver el contenido de tarjetas RFID previamente leídas o almacenadas en formato hexadecimal.		
<b>Fuente</b>	RUC-o6		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 111:** Requisito RSF-28 – Visualización en formato hexadecimal

<b>Identificador</b>	RSF-29	<b>Tipo</b>	Funcional
<b>Nombre</b>	Visualización como tarjeta de transporte		
<b>Descripción</b>	<p>La aplicación permitirá ver el contenido de tarjetas RFID previamente leídas o almacenadas como una tarjeta de transporte. Se mostrarán tres pestañas cada una con la siguiente información:</p> <ul style="list-style-type: none"> <li>• Pestaña “General”: <ul style="list-style-type: none"> <li>○ UID de la tarjeta.</li> <li>○ Tipo de tarjeta.</li> <li>○ Producto al que pertenece la tarjeta.</li> <li>○ Importe que posee la tarjeta.</li> </ul> </li> <li>• Pestaña “Historial de viaje”: <ul style="list-style-type: none"> <li>○ Identificador de viaje.</li> <li>○ Fecha del viaje.</li> <li>○ Hora del viaje.</li> <li>○ Compañía con la que se realiza el viaje.</li> <li>○ Tipo de transferencia. Puede ser: check-out, check-in o no-data.</li> <li>○ Identificador del vehículo utilizado.</li> <li>○ Identificador de la máquina utilizada.</li> <li>○ Importe empleado para realizar el viaje.</li> <li>○ Estación desde donde se inicial el viaje.</li> </ul> </li> <li>• Pestaña “Subscripciones”: <ul style="list-style-type: none"> <li>○ Identificador de la subscripción.</li> <li>○ Compañía de la subscripción.</li> <li>○ Fecha inicio de la subscripción.</li> <li>○ Fecha de caducidad de la subscripción.</li> <li>○ Descripción de la subscripción.</li> </ul> </li> </ul>		
<b>Fuente</b>	RUC-o6		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 112:** Requisito RSF-29 – Visualización como tarjeta de transporte

<b>Identificador</b>	RSF-30	<b>Tipo</b>	Funcional
<b>Nombre</b>	Visualización de condiciones de acceso		
<b>Descripción</b>	<p>La aplicación permitirá ver las condiciones de acceso de tarjetas RFID previamente leídas o almacenadas. Mostrará el tipo de clave necesaria (A o B) para realizar las operaciones de:</p> <ul style="list-style-type: none"> <li>• Lectura</li> <li>• Escritura</li> <li>• Incremento</li> <li>• Decremento</li> <li>• Transferencia</li> <li>• Restauración</li> </ul>		
<b>Fuente</b>	RUC-07		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 113:** Requisito RSF-30 – Visualización de condiciones de acceso

<b>Identificador</b>	RSF-31	<b>Tipo</b>	Funcional
<b>Nombre</b>	Importación de una tarjeta RFID		
<b>Descripción</b>	La aplicación permitirá importar una tarjeta RFID desde un fichero ubicado en el dispositivo.		
<b>Fuente</b>	RUC-08, RUR-07, RUR-17, RUR-24, RUR-31		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

**Tabla 114:** Requisito RSF-31 – Importación de una tarjeta RFID

<b>Identificador</b>	RSF-32	<b>Tipo</b>	Funcional
<b>Nombre</b>	Importación de varias tarjetas RFID		
<b>Descripción</b>	La aplicación permitirá importar varias tarjetas RFID desde un directorio ubicado en el dispositivo.		
<b>Fuente</b>	RUC-08, RUR-07, RUR-17, RUR-24, RUR-31		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

**Tabla 115:** Requisito RSF-32 – Importación de varias tarjetas RFID

<b>Identificador</b>	RSF-33	<b>Tipo</b>	Funcional
<b>Nombre</b>	Almacenamiento de claves en tarjetas importadas		
<b>Descripción</b>	La aplicación permitirá almacenar las claves pertenecientes a las tarjetas RFID que se importen.		
<b>Fuente</b>	RUC-08, RUR-08, RUR-15, RUR-16, RUR-24, RUR-31		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 116:** Requisito RSF-33 – Almacenamiento de claves en tarjetas importadas



<b>Identificador</b>	RSF-34	<b>Tipo</b>	Funcional
<b>Nombre</b>	Ruta importación de tarjetas RFID		
<b>Descripción</b>	Cada vez que se realiza una importación de tarjetas RFID la ruta del directorio es guardada para su siguiente ejecución.		
<b>Fuente</b>	RUC-o8		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

Tabla 117: Requisito RSF-34 – Ruta importación de tarjetas RFID

<b>Identificador</b>	RSF-35	<b>Tipo</b>	Funcional
<b>Nombre</b>	Estadísticas de uso		
<b>Descripción</b>	<p>La aplicación permitirá obtener unas estadísticas de uso sobre las claves utilizadas para la lectura y escritura de tarjetas RFID. La información mostrada es:</p> <ul style="list-style-type: none"> <li>• Clave.</li> <li>• Número de veces que la clave ha sido utilizada en lecturas.</li> <li>• Número de veces que la clave ha sido utilizada en escrituras.</li> <li>• Porcentaje de uso de la clave sobre el total de todas las claves.</li> </ul>		
<b>Fuente</b>	RUC-09, RUR-15, RUR-16, RUR-30, RUR-31, RUR-33		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 118: Requisito RSF-35 – Estadísticas de uso

<b>Identificador</b>	RSF-36	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de claves		
<b>Descripción</b>	La aplicación permitirá crear nuevas claves.		
<b>Fuente</b>	RUC-10, RUR-o8, RUR-15, RUR-16, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 119: Requisito RSF-36 – Creación de claves

<b>Identificador</b>	RSF-37	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de varias claves		
<b>Descripción</b>	Se podrán crear varias claves simultáneamente separándolas por saltos de línea.		
<b>Fuente</b>	RUC-10, RUR-o8, RUR-15, RUR-16, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 120: Requisito RSF-37 – Creación de varias claves

<b>Identificador</b>	RSF-38	<b>Tipo</b>	Funcional
<b>Nombre</b>	Modificación de claves		
<b>Descripción</b>	La aplicación permitirá modificar claves previamente creadas.		
<b>Fuente</b>	RUC-10, RUR-o8, RUR-15, RUR-16, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 121: Requisito RSF-38 – Modificación de claves

<b>Identificador</b>	RSF-39	<b>Tipo</b>	Funcional
<b>Nombre</b>	Eliminación de claves		
<b>Descripción</b>	La aplicación permitirá eliminar claves previamente creadas.		
<b>Fuente</b>	RUC-10, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 122:** Requisito RSF-39 – Eliminación de claves

<b>Identificador</b>	RSF-40	<b>Tipo</b>	Funcional
<b>Nombre</b>	Creación de grupo de claves		
<b>Descripción</b>	La aplicación permitirá crear grupos de claves de claves almacenadas previamente. Para almacenar un grupo de claves el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de grupo de claves</li> <li>• Incluir al menos una clave</li> </ul>		
<b>Fuente</b>	RUC-11, RUR-09, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 123:** Requisito RSF-40 – Creación de grupo de claves

<b>Identificador</b>	RSF-41	<b>Tipo</b>	Funcional
<b>Nombre</b>	Modificación de grupo de claves		
<b>Descripción</b>	La aplicación permitirá modificar grupos de claves previamente creados. Para almacenar un grupo de claves el usuario deberá haber rellenado la siguiente información: <ul style="list-style-type: none"> <li>• Nombre de grupo de claves</li> <li>• Incluir al menos una clave</li> </ul>		
<b>Fuente</b>	RUC-11, RUR-09, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 124:** Requisito RSF-41 – Modificación de grupo de claves

<b>Identificador</b>	RSF-42	<b>Tipo</b>	Funcional
<b>Nombre</b>	Eliminación de grupo de claves		
<b>Descripción</b>	La aplicación permitirá eliminar grupos de claves previamente creados.		
<b>Fuente</b>	RUC-11, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 125:** Requisito RSF-42 – Eliminación de grupo de claves

<b>Identificador</b>	RSF-43	<b>Tipo</b>	Funcional
<b>Nombre</b>	Importación de un fichero de claves		
<b>Descripción</b>	La aplicación permitirá importar claves desde un fichero ubicado en el dispositivo.		
<b>Fuente</b>	RUC-12, RUR-08, RUR-15, RUR-16, RUR-24, RUR-31		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

**Tabla 126:** Requisito RSF-43 – Importación de un fichero de claves

<b>Identificador</b>	RSF-44	<b>Tipo</b>	Funcional
<b>Nombre</b>	Importación de varios ficheros de claves		
<b>Descripción</b>	La aplicación permitirá importar varios ficheros de claves desde un directorio ubicado en el dispositivo.		
<b>Fuente</b>	RUC-12, RUR-08, RUR-15, RUR-16, RUR-24, RUR-31		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Media

**Tabla 127:** Requisito RSF-44 – Importación de varios ficheros de claves

<b>Identificador</b>	RSF-45	<b>Tipo</b>	Funcional
<b>Nombre</b>	Ruta importación de claves		
<b>Descripción</b>	Cada vez que se realiza una importación de claves la ruta del directorio es guardada para su siguiente ejecución.		
<b>Fuente</b>	RUC-12		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

**Tabla 128:** Requisito RSF-45 – Ruta importación de claves

<b>Identificador</b>	RSF-46	<b>Tipo</b>	Funcional
<b>Nombre</b>	Activación tecnología NFC		
<b>Descripción</b>	La aplicación permitirá activar la tecnología NFC al abrir o reanudar la aplicación si el dispositivo posee dicha tecnología y esta se encuentra desactivada.		
<b>Fuente</b>	RUC-13		
<b>Necesidad</b>	Opcional	<b>Prioridad</b>	Baja
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Baja

**Tabla 129:** Requisito RSF-46 – Activación tecnología NFC

<b>Identificador</b>	RSF-47	<b>Tipo</b>	Funcional
<b>Nombre</b>	Prevenir errores		
<b>Descripción</b>	La aplicación debe prevenir todos los errores posibles durante cualquier tipo operación.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUC-05, RUC-06, RUC-07, RUC-08, RUC-09, RUC-10, RUC-11, RUC-12, RUC-13		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 130:** Requisito RSF-47 – Prevenir errores

<b>Identificador</b>	RSF-48	<b>Tipo</b>	Funcional
<b>Nombre</b>	Informar de errores		
<b>Descripción</b>	La aplicación debe informar de todos los errores producidos durante cualquier tipo operación.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUC-05, RUC-06, RUC-07, RUC-08, RUC-09, RUC-10, RUC-11, RUC-12, RUC-13		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 131:** Requisito RSF-48 – Informar de errores

<b>Identificador</b>	RSF-49	<b>Tipo</b>	Funcional
<b>Nombre</b>	Responder ante errores		
<b>Descripción</b>	La aplicación debe reaccionar ante los posibles errores que puedan producirse durante la ejecución de cualquier tipo operación.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUC-05, RUC-06, RUC-07, RUC-08, RUC-09, RUC-10, RUC-11, RUC-12, RUC-13		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 132: Requisito RSF-49 – Responder ante errores

### 1.2.2. Requisitos no funcionales

Los requisitos no funcionales se encargan de definir las restricciones que afectan a los servicios o funciones de la aplicación. A continuación se muestran los relativos a este proyecto.

#### 1.2.2.1. Requisitos software no funcionales de operación

<b>Identificador</b>	RSFN-OP-01	<b>Tipo</b>	Operación
<b>Nombre</b>	Tipos de claves		
<b>Descripción</b>	Existen dos tipos de claves diferentes: <ul style="list-style-type: none"> <li>Claves por defecto: son las claves que posee la aplicación y que no pueden ser modificadas ni eliminadas.</li> <li>Claves personalizadas: son las claves que el usuario almacena en la base de datos de la aplicación.</li> </ul>		
<b>Fuente</b>	RUC-10, RUR-20		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 133: Requisito RSFN-OP-01 – Tipos de claves

<b>Identificador</b>	RSFN-OP-02	<b>Tipo</b>	Operación
<b>Nombre</b>	Comprobación al guardar tarjeta		
<b>Descripción</b>	Para guardar una tarjeta el sistema comprueba que el identificador introducido para ella no exista ya en la base de datos, si existe ofrece la opción de sobrescribirla o renombrarla.		
<b>Fuente</b>	RUC-01, RUC-05, RUC-08, RUR-07, RUR-17		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 134: Requisito RSFN-OP-02 – Comprobación al guardar tarjeta

<b>Identificador</b>	RSFN-OP-03	<b>Tipo</b>	Operación
<b>Nombre</b>	Formato de tarjeta Mifare Ultralight		
<b>Descripción</b>	Para guardar y ver el contenido en formato ASCII de una tarjeta RFID de tipo Mifare Ultralight la aplicación comprueba que el formato de esta sea de 16 páginas de 8 caracteres hexadecimales.		
<b>Fuente</b>	RUC-01, RUC-05, RUC-06, RUC-08, RUR-11		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 135: Requisito RSFN-OP-03 – Formato de tarjeta Mifare Ultralight

<b>Identificador</b>	RSFN-OP-04	<b>Tipo</b>	Operación
<b>Nombre</b>	Formato de tarjeta Mifare Classic Mini		
<b>Descripción</b>	Para guardar, ver el contenido en formato ASCII, ver como tarjeta de transporte y ver las condiciones de acceso de una tarjeta RFID de tipo Mifare Classic Mini la aplicación comprueba que el formato de esta sea de 5 sectores de 4 bloques, cada uno compuesto de 32 caracteres hexadecimales.		
<b>Fuente</b>	RUC-01, RUC-05, RUC-06, RUC-07, RUC-08, RUR-12		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 136: Requisito RSFN-OP-04 – Formato de tarjeta Mifare Classic Mini**

<b>Identificador</b>	RSFN-OP-05	<b>Tipo</b>	Operación
<b>Nombre</b>	Formato de tarjeta Mifare Classic 1K		
<b>Descripción</b>	Para guardar, ver el contenido en formato ASCII, ver como tarjeta de transporte y ver las condiciones de acceso de una tarjeta RFID de tipo Mifare Classic 1K la aplicación comprueba que el formato de esta sea de 16 sectores de 4 bloques, cada uno compuesto de 32 caracteres hexadecimales.		
<b>Fuente</b>	RUC-01, RUC-05, RUC-06, RUC-07, RUC-08, RUR-13		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 137: Requisito RSFN-OP-05 – Formato de tarjeta Mifare Classic 1K**

<b>Identificador</b>	RSFN-OP-06	<b>Tipo</b>	Operación
<b>Nombre</b>	Formato de tarjeta Mifare Classic 4K		
<b>Descripción</b>	Para guardar, ver el contenido en formato ASCII, ver como tarjeta de transporte y ver las condiciones de acceso de una tarjeta RFID de tipo Mifare Classic 4K la aplicación comprueba que el formato de esta sea de 40 sectores, los 32 primeros compuestos de 4 bloques y los 8 últimos de 16 bloques. En ambos casos cada bloque estará formado por 32 caracteres hexadecimales.		
<b>Fuente</b>	RUC-01, RUC-05, RUC-06, RUC-07, RUC-08, RUR-14		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 138: Requisito RSFN-OP-06 – Formato de tarjeta Mifare Classic 4K**

<b>Identificador</b>	RSFN-OP-07	<b>Tipo</b>	Operación
<b>Nombre</b>	Comprobación de tipo de tarjeta		
<b>Descripción</b>	Para ver el contenido en formato ASCII, ver como tarjeta de transporte y ver las condiciones de acceso de una tarjeta RFID la aplicación comprueba que el contenido de la tarjeta sea de tipo Mifare Classic (Mini, 1K o 4K).		
<b>Fuente</b>	RUC-06, RUC-07		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 139: Requisito RSFN-OP-07 – Comprobación de tipo de tarjeta**

<b>Identificador</b>	RSFN-OP-08	<b>Tipo</b>	Operación
<b>Nombre</b>	Comprobación al guardar clave		
<b>Descripción</b>	Para guardar una clave la aplicación comprueba que el identificador introducido no exista ya en la base de datos y que la clave tenga una longitud de 12 caracteres únicamente hexadecimales.		
<b>Fuente</b>	RUC-10, RUC-12, RUR-08, RUR-15, RUR-16, RUR-18, RUR-19, RUR-23, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 140: Requisito RSFN-OP-08 – Comprobación al guardar clave

<b>Identificador</b>	RSFN-OP-09	<b>Tipo</b>	Operación
<b>Nombre</b>	Comprobación al guardar grupo de claves		
<b>Descripción</b>	Para guardar un grupo de claves la aplicación comprueba que el identificador introducido no exista ya en la base de datos y que se haya incluido al menos una clave en el grupo.		
<b>Fuente</b>	RUC-11, RUR-09, RUR-19, RUR-23		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 141: Requisito RSFN-OP-09 – Comprobación al guardar grupo de claves

<b>Identificador</b>	RSFN-OP-10	<b>Tipo</b>	Operación
<b>Nombre</b>	Comprobación al guardar tipo de tarjeta		
<b>Descripción</b>	Para guardar un tipo de tarjeta la aplicación antes comprueba que el valor introducido no exista ya en la base de datos.		
<b>Fuente</b>	RUC-01, RUC-05, RUR-10, RUR-23		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 142: Requisito RSFN-OP-10 – Comprobación al guardar tipo de tarjeta

<b>Identificador</b>	RSFN-OP-11	<b>Tipo</b>	Operación
<b>Nombre</b>	Activación de tecnología NFC		
<b>Descripción</b>	Para activar la tecnología NFC la aplicación comprueba si el dispositivo posee dicha tecnología y si se encuentra desactivada. Si se cumplen ambas condiciones muestra la pantalla "Conexiones inalámbricas y redes" perteneciente a la sección "Ajustes" del teléfono.		
<b>Fuente</b>	RUC-13		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 143: Requisito RSFN-OP-11 – Activación de tecnología NFC

<b>Identificador</b>	RSFN-OP-12	<b>Tipo</b>	Operación
<b>Nombre</b>	Ignorar claves en lectura o escritura		
<b>Descripción</b>	Cuando se lee o escribe una tarjeta RFID, y esta es de tipo Mifare Ultralight, las claves seleccionadas para la operación serán ignoradas.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-02, RUR-03, RUR-04, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 144: Requisito RSFN-OP-12 – Ignorar claves en lectura o escritura

<b>Identificador</b>	RSFN-OP-13	<b>Tipo</b>	Operación
<b>Nombre</b>	Escritura en tarjetas Mifare Ultralight		
<b>Descripción</b>	Para escribir en una tarjeta RFID de tipo Mifare Ultralight la aplicación comprueba si esta es de solo lectura. Si es así la escritura es cancelada y se muestra el mensaje correspondiente.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-03, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 145: Requisito RSFN-OP-13 – Escritura en tarjetas Mifare Ultralight**

<b>Identificador</b>	RSFN-OP-14	<b>Tipo</b>	Operación
<b>Nombre</b>	Lectura y escritura de tarjetas Mifare Classic		
<b>Descripción</b>	Para leer o escribir en una tarjeta RFID de tipo Mifare Classic (Mini, 1K y 4K) la aplicación comprueba si se ha seleccionado alguna clave previamente. Si no es así la operación es cancelada y se muestra el mensaje correspondiente.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-02, RUR-03, RUR-04, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 146: Requisito RSFN-OP-14 – Lectura y escritura de tarjetas Mifare Classic**

<b>Identificador</b>	RSFN-OP-15	<b>Tipo</b>	Operación
<b>Nombre</b>	Autenticación en tarjetas Mifare Classic		
<b>Descripción</b>	Para leer o escribir en una tarjeta RFID de tipo Mifare Classic (Mini, 1K y 4K) la aplicación comprueba que cada uno de sus sectores puede ser autenticado por una clave de las seleccionadas anteriormente. Si no es así la operación es cancelada y se muestra el mensaje correspondiente.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-02, RUR-03, RUR-04, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 147: Requisito RSFN-OP-15 – Autenticación en tarjetas Mifare Classic**

<b>Identificador</b>	RSFN-OP-16	<b>Tipo</b>	Operación
<b>Nombre</b>	Escritura en tarjetas Mifare Classic		
<b>Descripción</b>	Para escribir en una tarjeta RFID de tipo Mifare Classic (Mini, 1K y 4K) la aplicación comprueba si la tarjeta destino posee la capacidad suficiente para el contenido a almacenar, si no es así la operación es cancelada y se muestra el mensaje correspondiente.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-02, RUR-03, RUR-04, RUR-24, RUR-31, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 148: Requisito RSFN-OP-16 – Escritura en tarjetas Mifare Classic**



<b>Identificador</b>	RSFN-OP-17	<b>Tipo</b>	Operación
<b>Nombre</b>	Conexión con tarjeta RFID		
<b>Descripción</b>	Para realizar cualquier operación sobre una tarjeta RFID la aplicación debe conectarse previamente a ella. Si se produce algún error la operación es cancelada y se muestra el mensaje correspondiente.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-02, RUR-03, RUR-04		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 149: Requisito RSFN-OP-17 – Conexión con tarjeta RFID

<b>Identificador</b>	RSFN-OP-18	<b>Tipo</b>	Operación
<b>Nombre</b>	Comprobar tipo de tarjeta en operaciones		
<b>Descripción</b>	Para realizar cualquier operación sobre una tarjeta RFID la aplicación comprueba que esta sea de tipo Mifare Ultralight o Mifare Classic (Mini, 1K o 4K). Si no es la operación es cancelada y muestra el mensaje correspondiente.		
<b>Fuente</b>	RUC-01, RUC-02, RUC-03, RUC-04, RUR-01, RUR-02, RUR-03, RUR-04		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 150: Requisito RSFN-OP-18 – Comprobar tipo de tarjeta en operaciones

<b>Identificador</b>	RSFN-OP-19	<b>Tipo</b>	Operación
<b>Nombre</b>	Claves almacenadas para lectura y escritura		
<b>Descripción</b>	Las claves utilizadas para la lectura y escritura de una tarjeta RFID de tipo Mifare Classic deben haber sido almacenadas previamente.		
<b>Fuente</b>	RUC-10, RUR-08, RUR-15, RUR-16, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 151: Requisito RSFN-OP-19 – Claves almacenadas para lectura y escritura

<b>Identificador</b>	RSFN-OP-20	<b>Tipo</b>	Operación
<b>Nombre</b>	Claves almacenadas para grupos de claves		
<b>Descripción</b>	Las claves utilizadas para crear grupos de claves deben haber sido almacenadas previamente.		
<b>Fuente</b>	RUC-10, RUR-08, RUR-15, RUR-16, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 152: Requisito RSFN-OP-20 – Claves almacenadas para grupos de claves

<b>Identificador</b>	RSFN-OP-21	<b>Tipo</b>	Operación
<b>Nombre</b>	Grupos de claves almacenados para lectura y escritura		
<b>Descripción</b>	Los grupos de claves utilizados para la lectura y escritura de una tarjeta RFID de tipo Mifare Classic deben haber sido almacenados previamente.		
<b>Fuente</b>	RUC-11, RUR-09, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 153: Requisito RSFN-OP-21 – Grupos de claves almacenados para lectura y escritura



<b>Identificador</b>	RSFN-OP-22	<b>Tipo</b>	Operación
<b>Nombre</b>	Nombre de ficheros de claves		
<b>Descripción</b>	Los ficheros de claves a importar deben tener la extensión .txt.		
<b>Fuente</b>	RUC-12, RUR-31		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 154: Requisito RSNF-OP-22 – Nombre de ficheros de claves

<b>Identificador</b>	RSFN-OP-23	<b>Tipo</b>	Operación
<b>Nombre</b>	Nombre de ficheros de tarjetas		
<b>Descripción</b>	<p>Los ficheros de tarjetas a importar deben tener la forma “nombre_tipo.dmp”, donde:</p> <ul style="list-style-type: none"> <li>• <b>Nombre:</b> hace referencia al nombre con el que se va a guardar la tarjeta en la base de datos.</li> <li>• <b>Tipo:</b> hace referencia al tipo de tarjeta que se va a importar. Puede ser: <ul style="list-style-type: none"> <li>○ <b>mfu:</b> tarjeta de tipo Mifare Ultralight.</li> <li>○ <b>mfcMini:</b> tarjeta de tipo Mifare Classic Mini.</li> <li>○ <b>mfc1k:</b> tarjeta de tipo Mifare Classic 1K.</li> <li>○ <b>mfc4k:</b> tarjeta de tipo Mifare Classic 4K.</li> </ul> </li> <li>• <b>Dmp:</b> extensión del archivo.</li> </ul>		
<b>Fuente</b>	RUC-o8, RUR-31		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 155: Requisito RSNF-OP-23 – Nombre de ficheros de tarjetas

<b>Identificador</b>	RSFN-OP-24	<b>Tipo</b>	Operación
<b>Nombre</b>	Formato de ficheros de claves		
<b>Descripción</b>	<p>El contenido de los ficheros de claves a importar deben cumplir las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>• Debe haber una única clave en cada línea.</li> <li>• Cada clave debe estar compuesta de 12 caracteres hexadecimales.</li> </ul>		
<b>Fuente</b>	RUC-12, RUR-15, RUR-16, RUR-31		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 156: Requisito RSNF-OP-24 – Formato de ficheros de claves

<b>Identificador</b>	RSFN-OP-25	<b>Tipo</b>	Operación
<b>Nombre</b>	Formato de ficheros de tarjetas		
<b>Descripción</b>	<p>Los ficheros de tarjetas RFID a importar deben tener todo su contenido en formato binario con su contenido ordenado de la siguiente manera:</p> <ul style="list-style-type: none"> <li>• Tarjetas Mifare Ultralight: de la página número 1 a la 16.</li> <li>• Tarjetas Mifare Classic Mini: del bloque número 1 al 20.</li> <li>• Tarjetas Mifare Classic 1K: del bloque número 1 al 64.</li> <li>• Tarjetas Mifare Classic 4K: del bloque número 1 al 256.</li> </ul>		
<b>Fuente</b>	RUC-o8, RUR-31		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 157: Requisito RSNF-OP-25 – Formato de ficheros de tarjetas

Identificador	RSFN-OP-26	Tipo	Operación
Nombre	Cálculo de estadísticas de uso		
Descripción	Para crear las estadísticas de uso el backend almacena cada clave junto con el número de veces que ha sido utilizada para lecturas y escrituras. Con todo esto se calcula el porcentaje de uso que posee cada clave con respecto al total de todas las claves y es mostrado en una tabla ordenada descendientemente según el valor de dicho porcentaje. Si se produce algún error durante el proceso el mensaje correspondiente es mostrado.		
Fuente	RUC-09, RUR-25, RUR-30, RUR-31, RUR-33		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 158: Requisito RSFN-OP-26 – Cálculo de estadísticas de uso

Identificador	RSFN-OP-27	Tipo	Operación
Nombre	Comprobación backend		
Descripción	Para guardar una clave en el backend antes se comprueba si esta ya existe, si es así se obtiene, se actualiza la información (incrementa el contador correspondiente si la operación ha sido de lectura o escritura) y se vuelve a enviar al backend. Si no se crea una clave nueva y se envía al backend. Una clave es almacenada en el backend cada vez que se realiza una lectura o escritura.		
Fuente	RUC-09, RUR-25, RUR-30, RUR-31, RUR-33		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 159: Requisito RSFN-OP-27 – Comprobación backend

Identificador	RSFN-OP-28	Tipo	Operación
Nombre	Búsqueda de tarjetas RFID		
Descripción	Para ver, modificar o eliminar una tarjeta RFID almacenada la aplicación busca su identificador en la base de datos, si existe devuelve su contenido o la elimina, respectivamente.		
Fuente	RUC-05, RUR-24		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 160: Requisito RSFN-OP-28 – Búsqueda de tarjetas RFID

Identificador	RSFN-OP-29	Tipo	Operación
Nombre	Búsqueda de claves		
Descripción	Para ver, modificar o eliminar una clave almacenada la aplicación busca su identificador en la base de datos, si existe devuelve su contenido o la elimina, respectivamente.		
Fuente	RUC-10, RUR-24		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 161: Requisito RSFN-OP-29 – Búsqueda de claves

<b>Identificador</b>	RSFN-OP-30	<b>Tipo</b>	Operación
<b>Nombre</b>	Búsqueda de grupos de claves		
<b>Descripción</b>	Para ver, modificar o eliminar un grupo de claves almacenado la aplicación busca su identificador en la base de datos, si existe devuelve su contenido o lo elimina, respectivamente.		
<b>Fuente</b>	RUC-11, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 162:** Requisito RSFN-OP-30 – Búsqueda de grupos de claves

<b>Identificador</b>	RSFN-OP-31	<b>Tipo</b>	Operación
<b>Nombre</b>	Listado de tarjetas		
<b>Descripción</b>	Para visualizar todas las tarjetas la aplicación obtiene todos los tipos de tarjetas almacenados, busca las tarjetas pertenecientes a cada uno de esos tipos y se agrupan las tarjetas de cada tipo en pestañas diferentes en la interfaz. Si no existen tarjetas de un determinado tipo muestra su mensaje de error correspondiente.		
<b>Fuente</b>	RUC-05, RUR-17, RUR-21, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 163:** Requisito RSFN-OP-31 – Listado de tarjetas

<b>Identificador</b>	RSFN-OP-32	<b>Tipo</b>	Operación
<b>Nombre</b>	Listado de claves		
<b>Descripción</b>	Para visualizar todas las claves la aplicación busca las claves por defecto y después las claves personalizadas.		
<b>Fuente</b>	RUC-10, RUR-24		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 164:** Requisito RSFN-OP-32 – Listado de claves

<b>Identificador</b>	RSFN-OP-33	<b>Tipo</b>	Operación
<b>Nombre</b>	Notificación de errores		
<b>Descripción</b>	Cuando el usuario comete un error la aplicación se lo notifica por medio de un mensaje emergente y le informa del error cometido.		
<b>Fuente</b>	RUR-35, RUR-37		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 165:** Requisito RSFN-OP-33 – Notificación de errores

### 1.2.2.2. Requisitos software no funcionales de interfaz

Identificador	RSFN-INT-01	Tipo	Interfaz
Nombre	Pantalla principal		
Descripción	<p>Existe una pantalla principal con:</p> <ul style="list-style-type: none"> <li>El icono principal de la aplicación en la barra de menú.</li> <li>Cinco botones con su imagen y texto correspondiente para realizar las siguientes acciones: <ul style="list-style-type: none"> <li>Leer tarjetas RFID.</li> <li>Escribir tarjetas RFID.</li> <li>Gestión de tarjetas RFID almacenadas.</li> <li>Gestión de claves y grupos de claves.</li> <li>Ver las estadísticas de uso de las claves.</li> </ul> </li> </ul>		
Fuente	RUC-01, RUC-02, RUC-03, RUC-04, RUC-05, RUC-06, RUC-07, RUC-08, RUC-09, RUC-10, RUC-11, RUC-12, RUC-13		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 166: Requisito RSFN-INT-01 – Pantalla principal

Identificador	RSFN-INT-02	Tipo	Interfaz
Nombre	Pantalla de selección de claves		
Descripción	<p>Existe una pantalla para seleccionar claves al realizar lecturas o escrituras de tarjetas RFID. Está compuesta por:</p> <ul style="list-style-type: none"> <li>El icono perteneciente a esta pantalla en la barra de menú.</li> <li>Una lista con las tres opciones de claves disponibles: <ul style="list-style-type: none"> <li>Sin claves: no utilizar ninguna clave para la operación.</li> <li>Todas las claves: todas las claves almacenadas son utilizadas para la operación.</li> <li>Grupos de claves: contiene un listado con los grupos de claves almacenados en el dispositivo. Se utilizan todas las claves de cada grupo para realizar la operación.</li> </ul> </li> <li>Botón que permite comenzar la lectura o escritura.</li> </ul>		
Fuente	RUC-02, RUC-04		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 167: Requisito RSFN-INT-02 – Pantalla de selección de claves

Identificador	RSFN-INT-03	Tipo	Interfaz
Nombre	Pantalla de espera		
Descripción	<p>Existe una pantalla para esperar la detección de una tarjeta RFID cuando se realiza una lectura o escritura. Está compuesta por:</p> <ul style="list-style-type: none"> <li>El icono perteneciente a esta pantalla en la barra de menú.</li> <li>Imagen de fondo indicando el método para detectar la tarjeta RFID con el dispositivo.</li> </ul>		
Fuente	RUC-01, RUC-03		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 168: Requisito RSFN-INT-03 – Pantalla de espera

Identificador	RSFN-INT-04	Tipo	Interfaz
Nombre	Pantalla de lectura/modificación/ver como hexadecimal/nueva tarjeta		
Descripción	<p>Existe una pantalla para la lectura/modificación/ver como hexadecimal/nueva tarjeta de una tarjeta RFID con:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Campo de texto para escribir el nombre de la tarjeta.</li> <li>• Desplegable para seleccionar el tipo de tarjeta.</li> <li>• Lista editable con el contenido de la tarjeta en formato hexadecimal. Esta lista está compuesta por los n elementos de la tarjeta (sectores y páginas para Mifare Classic y Mifare Ultralight, respectivamente). Todo el contenido es mostrado en mayúsculas.</li> <li>• Icono para guardar tarjeta en el dispositivo.</li> <li>• Las siguientes opciones en el menú desplegable: <ul style="list-style-type: none"> <li>○ Ver como tarjeta de transporte: ver el contenido de la tarjeta como una tarjeta de transporte.</li> <li>○ Ver como ASCII: ver contenido de la tarjeta en formato ASCII.</li> <li>○ Ver condiciones de acceso: ver condiciones de acceso de la tarjeta.</li> </ul> </li> </ul>		
Fuente	RUC-01, RUC-05, RUC-06, RUC-07, RUR-01, RUR-11, RUR-12, RUR-13, RUR-14		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

**Tabla 169:** Requisito RSFN-INT-04 – Pantalla de lectura/modificación/ver como hexadecimal/nueva tarjeta

Identificador	RSFN-INT-05	Tipo	Interfaz
Nombre	Pantalla de ver como ASCII		
Descripción	<p>Existe una pantalla para ver el contenido de la tarjeta RFID en formato ASCII formada por:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Campo de texto para escribir el nombre de la tarjeta.</li> <li>• Desplegable para seleccionar el tipo de tarjeta.</li> <li>• Lista editable con el contenido de la tarjeta en formato ASCII. Esta lista está compuesta por los n elementos de la tarjeta (sectores y páginas para Mifare Classic y Mifare Ultralight, respectivamente).</li> <li>• Icono para guardar tarjeta en el dispositivo.</li> <li>• La opción Ver como hexadecimal en el menú desplegable.</li> </ul>		
Fuente	RUC-06		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

**Tabla 170:** Requisito RSFN-INT-05 – Pantalla de ver como ASCII

<b>Identificador</b>	RSFN-INT-o6	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Pantalla de tarjeta de transporte		
<b>Descripción</b>	<p>Existe una pantalla para ver el contenido de una tarjeta Mifare Classic como una tarjeta de transporte. Esta pantalla está formada por:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• La pantalla está dividida en las siguientes tres pestañas: <ul style="list-style-type: none"> <li>○ General: formado por las columnas: <ul style="list-style-type: none"> <li>▪ UID: identificador de la tarjeta.</li> <li>▪ Tipo de tarjeta: puede ser Mifare Classic Mini, Mifare Classic 1K o Mifare Classic 4K.</li> <li>▪ Producto: hace referencia al producto al que pertenece esta tarjeta.</li> <li>▪ Importe: importe restante en la tarjeta.</li> </ul> </li> <li>○ Historial de viajes: contiene una tabla con los campos: <ul style="list-style-type: none"> <li>▪ ID: identificador del viaje.</li> <li>▪ Fecha: fecha del viaje.</li> <li>▪ Hora: hora del viaje.</li> <li>▪ Compañía: compañía con la que se realiza el viaje.</li> <li>▪ Transferencia: tipo de transferencia. Puede ser: check-out, check-in o no-data.</li> <li>▪ Vehículo: identificador del vehículo en el que se realiza el viaje.</li> <li>▪ Máquina: identificador de la máquina en la que se realiza el viaje.</li> <li>▪ Importe: gasto del viaje.</li> <li>▪ Estación: estación en la que se utiliza la tarjeta de transporte.</li> </ul> </li> <li>○ Suscripciones: contiene una tabla con los campos: <ul style="list-style-type: none"> <li>▪ ID: identificador de la suscripción.</li> <li>▪ Compañía: compañía de la suscripción.</li> <li>▪ Válido desde: fecha inicio de la suscripción.</li> <li>▪ Válido hasta: fecha caducidad de la suscripción.</li> <li>▪ Suscripción: descripción de la suscripción.</li> </ul> </li> </ul> </li> </ul>		
<b>Fuente</b>	RUC-o6		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 171: Requisito RSFN-INT-o6 – Pantalla de tarjeta de transporte

<b>Identificador</b>	RSN-INT-07	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Pantalla de condiciones de acceso		
<b>Descripción</b>	<p>Existe una pantalla para ver las condiciones de acceso de las tarjetas Mifare Classic. Esta pantalla está formada por:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Se muestra una tabla con la siguiente información: <ul style="list-style-type: none"> <li>○ Ubicación: hace referencia al sector, y dentro de este al bloque, a las propias condiciones de acceso y a las claves A y B.</li> <li>○ Lectura: clave necesaria para realizar esta operación.</li> <li>○ Escritura clave necesaria para realizar esta operación.</li> <li>○ Incremento: clave necesaria para realizar esta operación.</li> <li>○ Decremento/Transferencia/Restaurar: clave necesaria para realizar estas operaciones.</li> </ul> </li> </ul> <p>El valor de la clave puede tener uno de los siguientes valores:</p> <ul style="list-style-type: none"> <li>• Clave A: necesario autenticar el sector con la clave A para realizar la operación.</li> <li>• Clave B: necesario autenticar el sector con la clave B para realizar la operación.</li> <li>• Clave A B: necesario autenticar el sector con la clave A o B para realizar la operación.</li> <li>• Nunca: nunca va a poder realizarse la operación.</li> </ul>		
<b>Fuente</b>	RUC-07		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 172: Requisito RSNF-INT-07 – Pantalla de condiciones de acceso

<b>Identificador</b>	RSN-INT-08	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Pantalla de tarjetas para escribir		
<b>Descripción</b>	<p>Existe una pantalla para ver las tarjetas RFID almacenadas formada con:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Tantas pestañas como tipos de tarjetas se hayan almacenado.</li> <li>• En cada pestaña habrá un listado de las tarjetas RFID almacenadas y ordenadas por el nombre en orden ascendente para ese tipo de tarjeta.</li> <li>• En los listados solo se mostrará el nombre de la tarjeta con el que se ha almacenado.</li> </ul>		
<b>Fuente</b>	RUC-03		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

Tabla 173: Requisito RSNF-INT-08 – Pantalla de tarjetas para escribir

Identificador	RSFN-INT-09	Tipo	Interfaz
Nombre	Pantalla de tarjetas RFID		
Descripción	<p>Existe una pantalla para ver las tarjetas RFID almacenadas formada con:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Tantas pestañas como tipos de tarjetas se hayan almacenado junto con una primera pestaña donde se listarán todas las tarjetas.</li> <li>• En cada pestaña, excepto en la primera, habrá un listado de las tarjetas RFID almacenadas correspondientes a ese tipo de tarjeta.</li> <li>• Todos los listados estarán ordenados en orden ascendente por el nombre de la tarjeta.</li> <li>• En los listados solo se mostrará el nombre de la tarjeta, excepto en la primera pestaña que aparecerá junto con el tipo de tarjeta.</li> <li>• Las siguientes opciones en el menú desplegable: <ul style="list-style-type: none"> <li>○ Crear tag: crea y almacena una nueva tarjeta en el dispositivo.</li> <li>○ Importar tags: guardar en la base de datos tarjetas que actualmente se encuentran en ficheros dentro del dispositivo.</li> </ul> </li> </ul>		
Fuente	RUC-05, RUC-08		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 174: Requisito RSFN-INT-09 – Pantalla de tarjetas RFID

Identificador	RSFN-INT-10	Tipo	Interfaz
Nombre	Pantalla de claves y grupos de claves		
Descripción	<p>Existe una pantalla para ver las tarjetas RFID almacenadas formada con:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Dos pestañas: claves y grupos de claves. <ul style="list-style-type: none"> <li>○ Pestaña claves: contiene un listado con todas las claves almacenadas, el cual primero está relleno con las claves por defecto y a continuación con las personalizadas, ambas ordenadas de manera ascendente. Todas las claves son mostradas en mayúsculas.</li> <li>○ Pestaña de grupos de claves: contiene un listado con todos los grupos de claves almacenados. Se muestra el nombre del grupo junto con el número de claves que lo compone. La lista está ordenada por el nombre del grupo de manera ascendente.</li> </ul> </li> <li>• Icono para crear nuevas claves en el menú.</li> <li>• Las siguientes opciones en el menú desplegable: <ul style="list-style-type: none"> <li>○ Crear grupo de claves: crea y almacena un nuevo grupo de claves.</li> <li>○ Importar claves: guardar en la base de datos claves que actualmente se encuentran en ficheros dentro del dispositivo.</li> </ul> </li> </ul>		
Fuente	RUC-10, RUC-11, RUC-12		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 175: Requisito RSFN-INT-10 – Pantalla de claves y grupos de claves



Identificador	RSFN-INT-11	Tipo	Interfaz
Nombre	Pantalla de estadísticas		
Descripción	<p>Existe una pantalla para ver las estadísticas de uso de las claves. Esta pantalla está formada por:</p> <ul style="list-style-type: none"> <li>• El icono perteneciente a esta pantalla en la barra de menú.</li> <li>• Contiene una tabla con los campos: <ul style="list-style-type: none"> <li>○ Clave: hace referencia a la clave del backend. Su contenido se muestra en mayúsculas.</li> <li>○ Nº lecturas: indica el número de veces con las que se ha leído alguna información con esta clave.</li> <li>○ Nº escrituras: indica el número de veces con las que se ha escrito alguna información en una tarjeta RFID con esta clave.</li> <li>○ Porcentaje: indica el porcentaje de uso total de esta clave con respecto al uso de todas las claves almacenadas en el backend.</li> </ul> </li> </ul>		
Fuente	RUC-09		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 176: Requisito RSFN-INT-11 – Pantalla de estadísticas

Identificador	RSFN-INT-12	Tipo	Interfaz
Nombre	Diálogo de espera		
Descripción	<p>Existe un diálogo que se mostrará mientras se lee o escribe una tarjeta RFID y durante la carga de las estadísticas de uso de las claves. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Icono de carga.</li> <li>• Mensaje que indica al usuario que debe esperar hasta que termine la tarea.</li> </ul>		
Fuente	RUC-01, RUC-03, RUC-09, RUR-01, RUR-03		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 177: Requisito RSFN-INT-12 – Diálogo de espera

Identificador	RSFN-INT-13	Tipo	Interfaz
Nombre	Diálogo de tarjeta repetida		
Descripción	<p>Existe un diálogo que se mostrará cuando se intente almacenar una tarjeta con un identificador ya existente en la base de datos. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Nombre de la tarjeta mostrado como título.</li> <li>• Mensaje indicando que la tarjeta ya existe.</li> <li>• Un botón para renombrar la tarjeta.</li> <li>• Un botón para reemplazar la tarjeta.</li> </ul>		
Fuente	RUC-01, RUC-05, RUR-07		
Necesidad	Esencial	Prioridad	Alta
Estabilidad	Estable	Verificabilidad	Alta

Tabla 178: Requisito RSFN-INT-13 – Diálogo de tarjeta repetida

<b>Identificador</b>	RSFN-INT-14	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para renombrar tarjeta		
<b>Descripción</b>	<p>Existe un diálogo que se mostrará para renombrar una tarjeta y almacenarla en la base de datos. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto para reescribir el identificador de la tarjeta.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y almacenar la tarjeta.</li> </ul>		
<b>Fuente</b>	RUC-01, RUC-05, RUR-07		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 179: Requisito RSFN-INT-14 – Diálogo para renombrar tarjeta**

<b>Identificador</b>	RSFN-INT-15	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para eliminar tarjeta		
<b>Descripción</b>	<p>Existe un diálogo que se mostrará para eliminar una tarjeta de la base de datos. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Título relleno con el nombre de la tarjeta a eliminar.</li> <li>• Mensaje preguntando si de verdad se quiere eliminar la tarjeta.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y eliminar la tarjeta.</li> </ul>		
<b>Fuente</b>	RUC-05		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 180: Requisito RSFN-INT-15 – Diálogo para eliminar tarjeta**

<b>Identificador</b>	RSFN-INT-16	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para crear tarjeta		
<b>Descripción</b>	<p>Existe un diálogo para crear una nueva tarjeta. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Título indicando que se debe seleccionar el tipo de tarjeta a crear.</li> <li>• Un listado con los siguientes cuatro tipos: <ul style="list-style-type: none"> <li>○ Mifare Ultralight: tarjeta de 16 páginas.</li> <li>○ Mifare Classic Mini: tarjeta de 5 sectores y 4 bloques en cada uno de ellos.</li> <li>○ Mifare Classic 1K: tarjeta de 16 sectores y 4 bloques en cada uno de ellos.</li> <li>○ Mifare Classic 4K: tarjeta de 40 sectores, los 32 primeros con 4 bloques y los 8 últimos con 16 bloques.</li> </ul> </li> </ul>		
<b>Fuente</b>	RUC-05		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 181: Requisito RSFN-INT-16 – Diálogo para crear tarjeta**

<b>Identificador</b>	RSFN-INT-17	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para crear clave		
<b>Descripción</b>	Existe un diálogo para crear y almacenar una clave en la base de datos. Este diálogo está compuesto por: <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto para escribir la nueva clave.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y almacenar la clave.</li> </ul>		
<b>Fuente</b>	RUC-10		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 182:** Requisito RSFN-INT-17 – Diálogo para crear clave

<b>Identificador</b>	RSFN-INT-18	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para modificar clave		
<b>Descripción</b>	Existe un diálogo para modificar una clave ya existente en la base de datos. Este diálogo está compuesto por: <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto editable relleno con la clave que se quiere modificar.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y almacenar la clave.</li> </ul>		
<b>Fuente</b>	RUC-10		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 183:** Requisito RSFN-INT-18 – Diálogo para modificar clave

<b>Identificador</b>	RSFN-INT-19	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para eliminar clave		
<b>Descripción</b>	Existe un diálogo para eliminar una clave de la base de datos. Este diálogo está compuesto por: <ul style="list-style-type: none"> <li>• Título relleno con la clave a eliminar.</li> <li>• Mensaje preguntando si de verdad se quiere eliminar la clave.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y eliminar la clave.</li> </ul>		
<b>Fuente</b>	RUC-10		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 184:** Requisito RSFN-INT-19 – Diálogo para eliminar clave

<b>Identificador</b>	RSFN-INT-20	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para crear grupo de claves		
<b>Descripción</b>	<p>Existe un diálogo para crear y almacenar un grupo de claves en la base de datos. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto para escribir el nombre del nuevo grupo de claves.</li> <li>• Listado de todas las claves almacenadas y que se pueden seleccionar para incluirlas en el grupo.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y almacenar el grupo de claves.</li> </ul>		
<b>Fuente</b>	RUC-11		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 185:** Requisito RSFN-INT-20 – Diálogo para crear grupo de claves

<b>Identificador</b>	RSFN-INT-21	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para modificar grupo de claves		
<b>Descripción</b>	<p>Existe un diálogo para modificar una clave ya existente en la base de datos. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto editable relleno con el nombre del grupo de claves que se quiere modificar.</li> <li>• Listado de todas las claves almacenadas y que se pueden seleccionar para incluirlas en el grupo. Están seleccionadas aquellas que actualmente pertenecen al grupo.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y almacenar el grupo de claves.</li> </ul>		
<b>Fuente</b>	RUC-11		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 186:** Requisito RSFN-INT-21 – Diálogo para modificar grupo de claves

<b>Identificador</b>	RSFN-INT-22	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para eliminar grupo de claves		
<b>Descripción</b>	<p>Existe un diálogo para eliminar una clave de la base de datos. Este diálogo está compuesto por:</p> <ul style="list-style-type: none"> <li>• Título relleno con el nombre del grupo de claves.</li> <li>• Mensaje preguntando si de verdad se quiere eliminar el grupo.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación y eliminar el grupo.</li> </ul>		
<b>Fuente</b>	RUC-11		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 187:** Requisito RSFN-INT-22 – Diálogo para eliminar grupo de claves

<b>Identificador</b>	RSFN-INT-23	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para importar tarjetas		
<b>Descripción</b>	Existe un diálogo para importar tarjetas. Este diálogo está compuesto por: <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto editable relleno con la dirección de la última importación, o en su defecto la dirección por defecto.</li> <li>• Opción para guardar las claves de las tarjetas importadas.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación e importar las tarjetas.</li> </ul>		
<b>Fuente</b>	RUC-o8		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 188:** Requisito RSFN-INT-23 – Diálogo para importar tarjetas

<b>Identificador</b>	RSFN-INT-24	<b>Tipo</b>	Interfaz
<b>Nombre</b>	Diálogo para importar claves		
<b>Descripción</b>	Existe un diálogo para importar claves. Este diálogo está compuesto por: <ul style="list-style-type: none"> <li>• Título de la acción.</li> <li>• Campo de texto editable relleno con la dirección de la última importación, o en su defecto la dirección por defecto.</li> <li>• Un botón para cancelar la operación.</li> <li>• Un botón para aceptar la operación e importar las claves.</li> </ul>		
<b>Fuente</b>	RUC-12		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 189:** Requisito RSFN-INT-24 – Diálogo para importar claves

### 1.2.2.3. Requisitos software no funcionales de recursos

<b>Identificador</b>	RSFN-REC-01	<b>Tipo</b>	Recurso
<b>Nombre</b>	Espacio de almacenamiento		
<b>Descripción</b>	El espacio mínimo en disco necesario para la aplicación será de 7 Mb.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 190:** Requisito RSFN-REC-01 – Espacio de almacenamiento

<b>Identificador</b>	RSFN-REC-02	<b>Tipo</b>	Recurso
<b>Nombre</b>	Memoria principal		
<b>Descripción</b>	La memoria principal mínima necesaria para el correcto funcionamiento de la aplicación será de 512 Mb.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 191:** Requisito RSFN-REC-02 – Memoria principal

<b>Identificador</b>	RSFN-REC-03	<b>Tipo</b>	Recurso
<b>Nombre</b>	Velocidad del procesador		
<b>Descripción</b>	El dispositivo debe poseer un procesador con una velocidad mínima de 800 Mhz.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 192:**            **Requisito RSFN-REC-03 – Velocidad del procesador**

<b>Identificador</b>	RSFN-REC-04	<b>Tipo</b>	Recurso
<b>Nombre</b>	Tecnología NFC		
<b>Descripción</b>	El dispositivo debe poseer la tecnología NFC para realizar operaciones sobre tarjetas RFID.		
<b>Fuente</b>	RUC-1, RUC-03, RUC-13, RUR-01, RUR-03, RUR-34		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 193:**            **Requisito RSFN-REC-04 – Tecnología NFC**

<b>Identificador</b>	RSFN-REC-05	<b>Tipo</b>	Recurso
<b>Nombre</b>	Tecnología de red		
<b>Descripción</b>	El dispositivo debe poseer conectividad Wifi o 3G para poder acceder al backend.		
<b>Fuente</b>	RUC-09, RUR-25, RUR-33		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 194:**            **Requisito RSFN-REC-05 – Tecnología de red**

#### **1.2.2.4.    Requisitos software no funcionales de rendimiento**

<b>Identificador</b>	RSFN-REN-01	<b>Tipo</b>	Rendimiento
<b>Nombre</b>	Tiempos de respuesta		
<b>Descripción</b>	Cualquier operación realizada en la aplicación tardará en responder un máximo de 5 segundos, a excepción de la lectura y escritura de tarjetas RFID y la primera operación tras su instalación.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 195:**            **Requisito RSFN-REN-01 – Tiempos de respuesta**

<b>Identificador</b>	RSFN-REN-02	<b>Tipo</b>	Rendimiento
<b>Nombre</b>	Tiempo de respuesta en primera operación		
<b>Descripción</b>	La primera operación realizada tras la instalación tardará en responder un máximo de 10 segundos debido a que debe actualizar la base de datos.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 196:**            **Requisito RSFN-REN-02 – Tiempo de respuesta en primera operación**

<b>Identificador</b>	RSFN-REN-03	<b>Tipo</b>	Rendimiento
<b>Nombre</b>	Tiempos de respuesta en Mifare Ultralight		
<b>Descripción</b>	Las operaciones de lectura y escritura en tarjetas RFID de tipo Mifare Ultralight tardarán en responder un máximo de 3 segundos.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 197:**                    **Requisito RSNF-REN-03 – Tiempos de respuesta en Mifare Ultralight**

<b>Identificador</b>	RSFN-REN-04	<b>Tipo</b>	Rendimiento
<b>Nombre</b>	Tiempos de respuesta en Mifare Classic		
<b>Descripción</b>	El tiempo necesario para realizar operaciones de lectura y escritura en tarjetas RFID de tipo Mifare Classic (Mini, 1K y 4K) será proporcional al número de claves seleccionadas y al tamaño de la tarjeta.		
<b>Fuente</b>	RUR-35		
<b>Necesidad</b>	Esencial	<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable	<b>Verificabilidad</b>	Alta

**Tabla 198:**                    **Requisito RSNF-REN-04 – Tiempos de respuesta en Mifare Classic**

1.3. Matrices de trazabilidad

1.3.1. Matriz de trazabilidad entre requisitos de usuario y requisitos software funcionales

	RUC-01	RUC-02	RUC-03	RUC-04	RUC-05	RUC-06	RUC-07	RUC-08	RUC-09	RUC-10	RUC-11	RUC-12	RUC-13	RUR-01	RUR-02	RUR-03	RUR-04	RUR-05	RUR-06	RUR-07	RUR-08	RUR-09	RUR-10	RUR-11	RUR-12	RUR-13	RUR-14	RUR-15	RUR-16	RUR-17	RUR-18	RUR-19	RUR-20	RUR-21	RUR-22	RUR-23	RUR-24	RUR-25	RUR-26	RUR-27	RUR-28	RUR-29	RUR-30	RUR-31	RUR-32	RUR-33	RUR-34	RUR-35	RUR-36	RUR-37
RSF-01	X													X					X				X					X					X					X				X								
RSF-02	X													X	X				X				X					X					X					X				X								
RSF-03	X													X	X				X							X		X					X				X				X				X					
RSF-04	X													X	X				X									X		X			X				X				X				X					
RSF-05	X																						X													X														
RSF-06	X			X																																														
RSF-07	X			X																																														
RSF-08	X																																																	
RSF-09	X																																					X												
RSF-10	X																																					X												
RSF-11	X																																																	
RSF-12		X														X		X	X																	X					X			X						
RSF-13		X														X	X	X	X																	X					X			X						
RSF-14		X														X	X	X	X																	X					X			X						
RSF-15		X														X	X	X	X																	X					X			X						
RSF-16			X																																		X													
RSF-17			X																																		X													
RSF-18			X																																															
RSF-19																																						X				X	X		X					
RSF-20				X															X					X	X	X	X		X							X														
RSF-21				X																																	X													
RSF-22				X															X				X					X								X														



[illegible]

	RUC-01	RUC-02	RUC-03	RUC-04	RUC-05	RUC-06	RUC-07	RUC-08	RUC-09	RUC-10	RUC-11	RUC-12	RUC-13	RUR-01	RUR-02	RUR-03	RUR-04	RUR-05	RUR-06	RUR-07	RUR-08	RUR-09	RUR-10	RUR-11	RUR-12	RUR-13	RUR-14	RUR-15	RUR-16	RUR-17	RUR-18	RUR-19	RUR-20	RUR-21	RUR-22	RUR-23	RUR-24	RUR-25	RUR-26	RUR-27	RUR-28	RUR-29	RUR-30	RUR-31	RUR-32	RUR-33	RUR-34	RUR-35	RUR-36	RUR-37
RSF-48	X	X	X	X	X	X	X	X	X	X	X	X	X																																					
RSF-49	X	X	X	X	X	X	X	X	X	X	X	X	X																																					

Tabla 199: Matriz de trazabilidad entre requisitos de usuario y requisitos software funcionales

1.3.2. Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de operación

	RUC-01	RUC-02	RUC-03	RUC-04	RUC-05	RUC-06	RUC-07	RUC-08	RUC-09	RUC-10	RUC-11	RUC-12	RUC-13	RUR-01	RUR-02	RUR-03	RUR-04	RUR-05	RUR-06	RUR-07	RUR-08	RUR-09	RUR-10	RUR-11	RUR-12	RUR-13	RUR-14	RUR-15	RUR-16	RUR-17	RUR-18	RUR-19	RUR-20	RUR-21	RUR-22	RUR-23	RUR-24	RUR-25	RUR-26	RUR-27	RUR-28	RUR-29	RUR-30	RUR-31	RUR-32	RUR-33	RUR-34	RUR-35	RUR-36	RUR-37
RSFN-OP-01	X										X																																							
RSFN-OP-02	X				X			X											X											X																				
RSFN-OP-03	X				X	X		X																X																										
RSFN-OP-04	X				X	X	X	X																	X																									
RSFN-OP-05	X				X	X	X	X																		X																								
RSFN-OP-06	X				X	X	X	X																			X																							
RSFN-OP-07						X	X																																											
RSFN-OP-08										X		X									X							X	X		X	X					X	X												
RSFN-OP-09											X											X									X								X											
RSFN-OP-10	X				X																		X																											
RSFN-OP-11													X																																					
RSFN-OP-12	X	X	X	X										X	X	X	X																			X							X			X				
RSFN-OP-13	X	X	X	X										X		X																					X							X			X			
RSFN-OP-14	X	X	X	X										X	X	X	X																				X							X			X			
RSFN-OP-15	X	X	X	X										X	X	X	X																				X							X			X			
RSFN-OP-16	X	X	X	X										X	X	X	X																				X							X			X			
RSFN-OP-17	X	X	X	X										X	X	X	X																																	

[illegible]

**Tabla 200: Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de operación**

1.3.3. Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de interfaz

	RUC-01	RUC-02	RUC-03	RUC-04	RUC-05	RUC-06	RUC-07	RUC-08	RUC-09	RUC-10	RUC-11	RUC-12	RUC-13	RUR-01	RUR-02	RUR-03	RUR-04	RUR-05	RUR-06	RUR-07	RUR-08	RUR-09	RUR-10	RUR-11	RUR-12	RUR-13	RUR-14	RUR-15	RUR-16	RUR-17	RUR-18	RUR-19	RUR-20	RUR-21	RUR-22	RUR-23	RUR-24	RUR-25	RUR-26	RUR-27	RUR-28	RUR-29	RUR-30	RUR-31	RUR-32	RUR-33	RUR-34	RUR-35	RUR-36	RUR-37	
RSFN-INT-01	X	X	X	X	X	X	X	X	X	X	X	X	X																																						
RSFN-INT-02		X		X																																															
RSFN-INT-03	X		X																																																
RSFN-INT-04	X				X	X	X							X										X	X	X	X																								
RSFN-INT-05						X																																													
RSFN-INT-06						X																																													
RSFN-INT-07							X																																												
RSFN-INT-08			X																																																
RSFN-INT-09					X																																														
RSFN-INT-10										X	X	X																																							
RSFN-INT-11									X																																										
RSFN-INT-12	X		X						X					X	X																																				
RSFN-INT-13	X				X															X																															
RSFN-INT-14	X				X															X																															
RSFN-INT-15					X																																														
RSFN-INT-16					X																																														
RSFN-INT-17										X																																									
RSFN-INT-18										X																																									
RSFN-INT-19										X																																									
RSFN-INT-20											X																																								
RSFN-INT-21											X																																								
RSFN-INT-22											X																																								
RSFN-INT-23							X																																												
RSFN-INT-24												X																																							

Tabla 201: Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de interfaz

#### 1.3.4. Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de recursos

	RUC-01	RUC-02	RUC-03	RUC-04	RUC-05	RUC-06	RUC-07	RUC-08	RUC-09	RUC-10	RUC-11	RUC-12	RUC-13	RUR-01	RUR-02	RUR-03	RUR-04	RUR-05	RUR-06	RUR-07	RUR-08	RUR-09	RUR-10	RUR-11	RUR-12	RUR-13	RUR-14	RUR-15	RUR-16	RUR-17	RUR-18	RUR-19	RUR-20	RUR-21	RUR-22	RUR-23	RUR-24	RUR-25	RUR-26	RUR-27	RUR-28	RUR-29	RUR-30	RUR-31	RUR-32	RUR-33	RUR-34	RUR-35	RUR-36	RUR-37																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
RSFN-REC-01																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														

**Tabla 202: Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de recursos**

### 1.3.5. Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de rendimiento

[illegible]

**Tabla 203: Matriz de trazabilidad entre requisitos de usuario y requisitos software no funcionales de rendimiento**

## 2. Diseño

### 2.1. Arquitectura

En esta sección se van a detallar las distintas alternativas de diseño estudiadas para el desarrollo de la aplicación y posteriormente mostrar y explicar el diagrama de componentes del diseño escogido.

#### 2.1.1. Alternativas de diseño

El sistema abordado en este proyecto separa su contenido en tres componentes: los datos de la aplicación, la interfaz de usuario y la lógica de control.

- **Datos de la aplicación:** relacionado con el manejo de la base de datos: consulta, inserción, modificación y eliminación de información.
- **Interfaz de usuario:** encargado de la presentación de la aplicación y de gestionar los eventos que puedan ocurrir en la aplicación: mensajes recibidos del usuario, flujo de aplicación y control de navegación entre ventanas.
- **Lógica de control:** controla los eventos internos recibidos desde la interfaz de usuario y las acciones relacionadas con la modificación de la información del backend externo.

Desde el primer momento se decidió utilizar el patrón de arquitectura software Modelo-Vista-Controlador (MVC) moderno debido a que sus componentes modelo, vista y controlador se acoplan perfectamente a datos de la aplicación, interfaz de usuario y lógica de control, respectivamente.

A este patrón de arquitectura se le añadió la comunicación entre el componente Modelo y el backend externo para realizar las operaciones correspondientes sobre este.

### 2.1.2. Diagrama de componentes

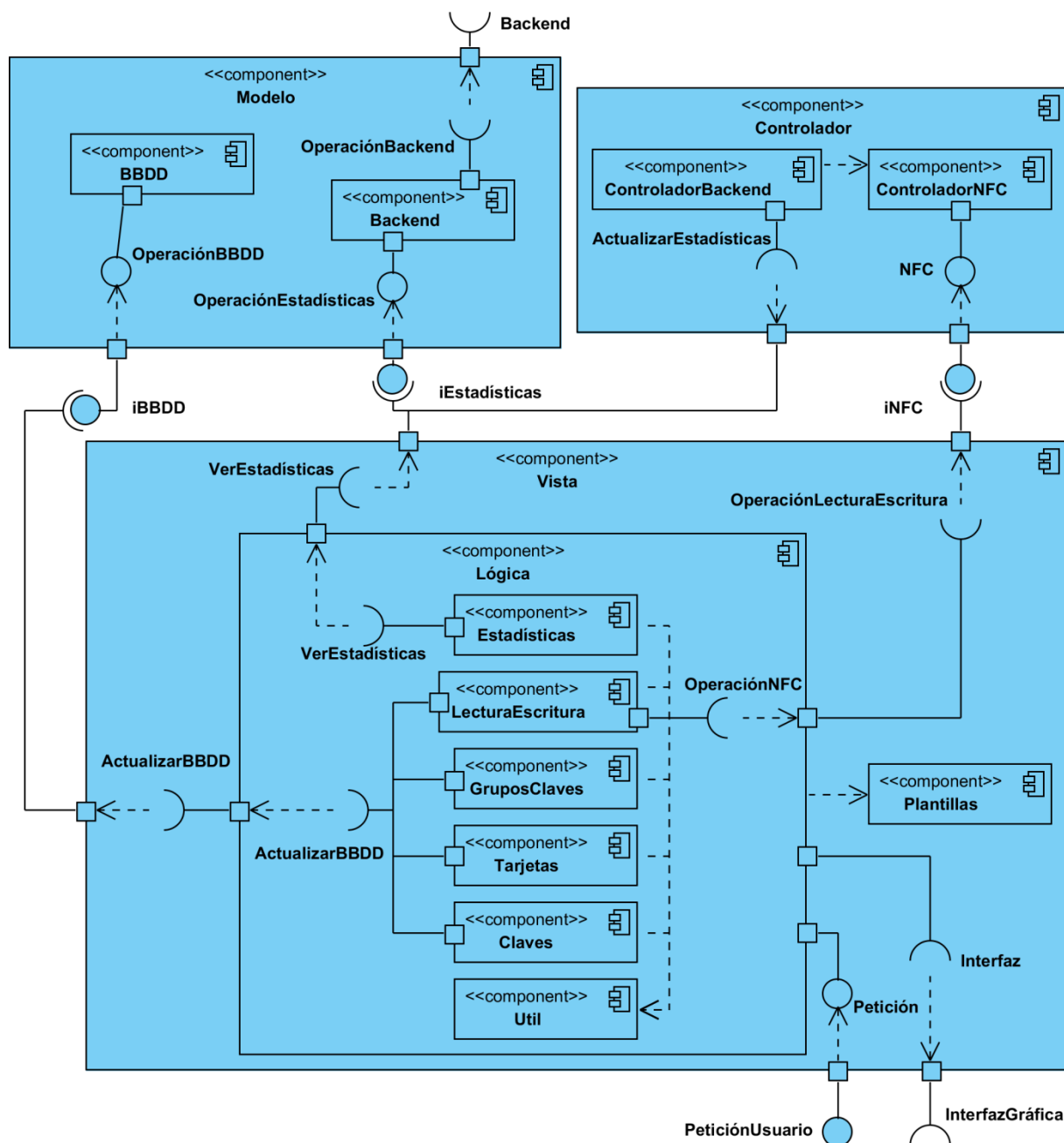


Ilustración 16: Diagrama de componentes

En la figura anterior se muestra el diagrama de componentes del sistema donde se pueden distinguir tres componentes principales: Modelo, Vista y Controlador.

A continuación se va a explicar cada uno de los componentes principales describiendo cada uno los subcomponentes que lo forman.

- **Modelo:** es el paquete encargado de la lógica de negocio y de la comunicación con la base de datos interna del sistema. Se ha utilizado el lenguaje SQLite para crear una base de datos relacional y trabajar con los datos de la aplicación. También se

encarga de realizar las operaciones sobre el backend externo. Está compuesto por los subcomponentes Backend y BBDD.

- **Backend:** contiene la funcionalidad necesaria para conectarse con el backend, realizar las operaciones solicitadas y devolver su resultado.
- **BBDD:** se encarga de todas las operaciones relacionadas de la base datos interna de la aplicación. Cuando le llega una solicitud crea su instrucción correspondiente en lenguaje SQLite, la ejecuta y devuelve el resultado correspondiente de esa operación.
- **Vista:** es el paquete encargado de la representación de la información y su lógica. Android utiliza plantillas XML para definir toda la información relativa a las interfaces y así poder añadir, modificar o eliminar elementos fácilmente. Controla los eventos recibidos del usuario y responde a sus peticiones. Está formado por los subcomponentes Plantillas y Lógica.
  - **Plantillas:** este subcomponente alberga todas las plantillas diseñadas para cada una de las interfaces de la aplicación.
  - **Lógica:** este subcomponente se encarga de la lógica necesaria en la vista y de controlar las peticiones del usuario. Está compuesto por los subcomponentes Estadísticas, LecturaEscritura, GruposClaves, Tarjetas, Claves y Util.
    - **Estadísticas:** se encarga de enviar la petición adecuada para obtener la información de estadísticas del backend externo y mostrarla a través de la interfaz.
    - **LecturaEscritura:** se encarga de gestionar las peticiones de lectura y escritura y manda dichas peticiones al subpaquete ControladorNFC (del componente Controlador), para que sean llevadas a cabo. También se encarga de mandar la petición adecuada para que una tarjeta ya leída sea almacenada en la BBDD.
    - **GruposClaves:** gestiona las peticiones sobre la creación, modificación y eliminación de grupos de claves en el sistema.
    - **Tarjetas:** gestiona las peticiones sobre la creación, modificación y eliminación de tarjetas en el sistema.
    - **Claves:** gestiona las peticiones relacionadas con la creación, modificación y eliminación de claves en el sistema.



- **Util:** contiene toda la funcionalidad en común para el resto de subcomponentes del componente Lógica.
- **Controlador:** este componente se ocupa de controlar los eventos recibidos desde el componente Vista, realizar las operaciones NFC y actualizar la información del backend. Está formado por los subcomponentes ControladorBackend y ControladorNFC.
  - **ControladorBackend:** encargado de gestionar las peticiones con el fin de actualizar la información ubicada en el backend externo. Depende del componente ControladorNFC ya que la información del backend solo es actualizada si se realiza alguna acción correcta sobre tarjetas RFID.
  - **ControladorNFC:** encargado de realizar las operaciones de lectura, escritura y autenticación entre el dispositivo y las tarjetas RFID. También se ocupa de reabrir y cerrar las conexiones con una tarjeta cuando es necesario.

## 2.2. Diagrama de clases

En este apartado se muestran las relaciones existentes entre las clases que forman los componentes de la aplicación.

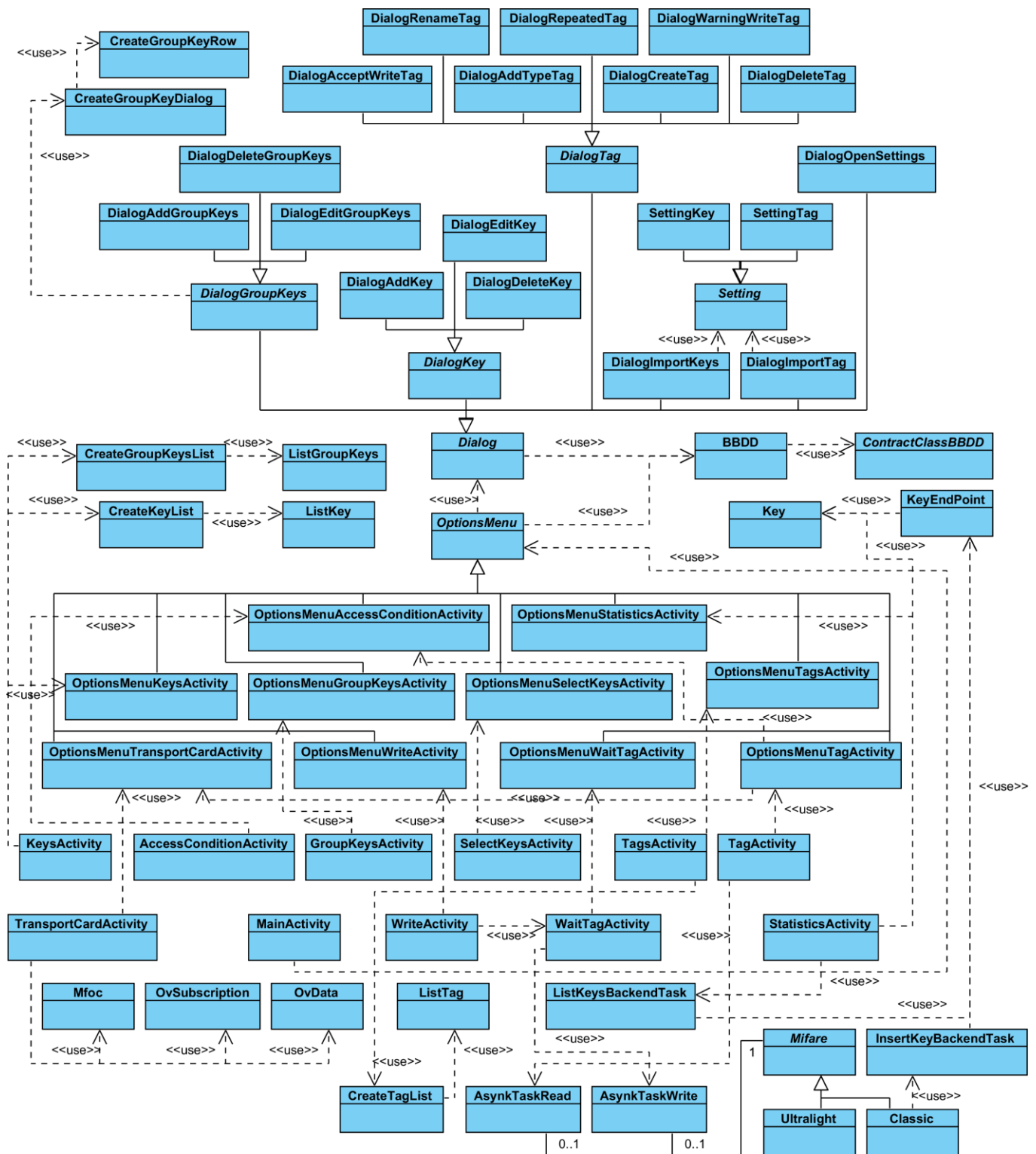


Ilustración 17: Diagrama de clases

### 2.3. Diseño de base de datos

En esta subsección se va a ilustrar y a explicar el diseño de la base de datos utilizado durante el desarrollo del sistema.

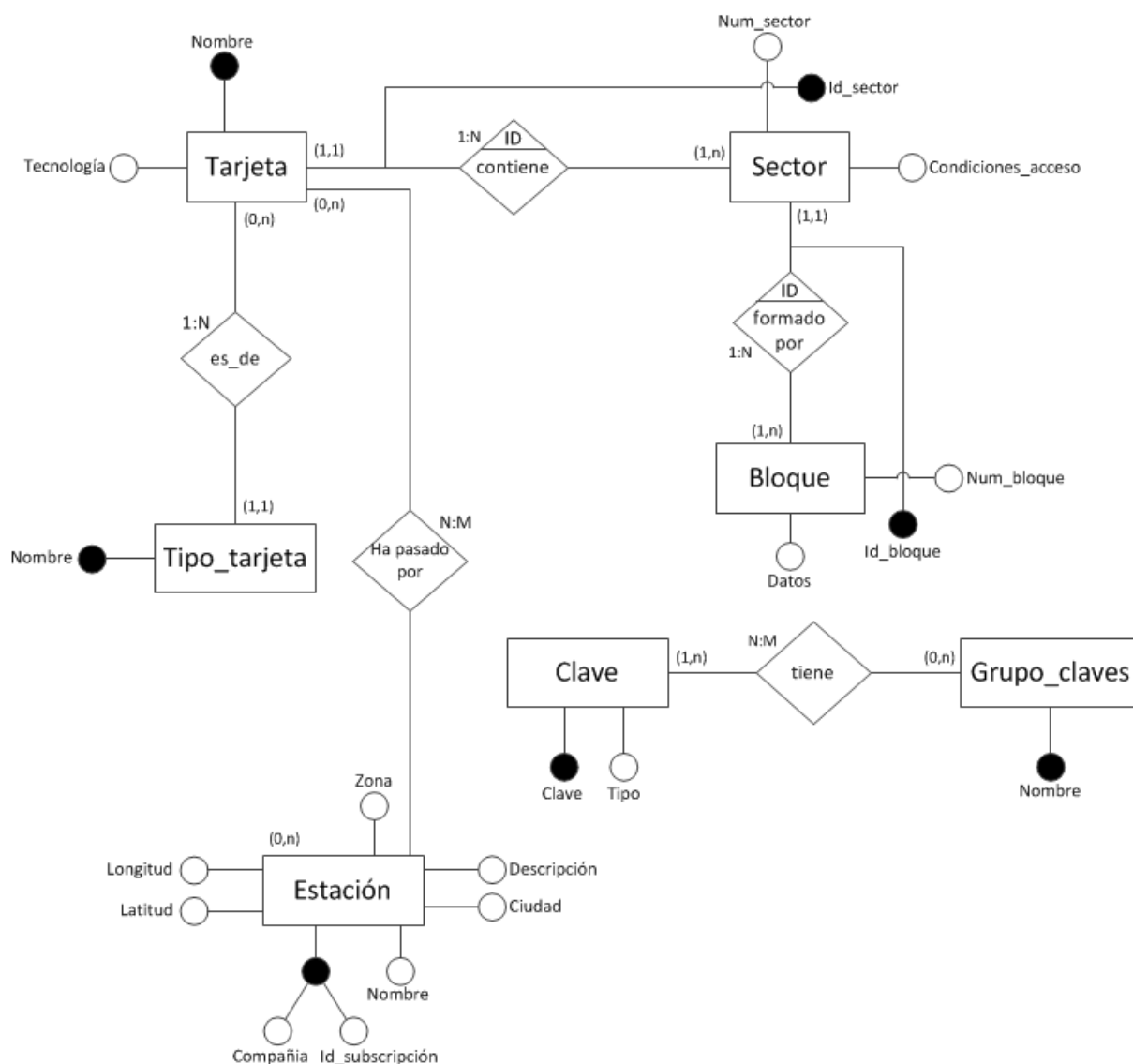


Ilustración 18: Modelo de datos del sistema

En la figura anterior se puede observar el modelo entidad-relación de la base de datos del sistema. En él se presentan las distintas entidades de la base de datos con sus atributos y relaciones correspondientes.

En la base de datos de la aplicación se almacena la información relevante de las tarjetas RFID. Cada tarjeta pertenece a un determinado tipo de tecnología (Mifare Ultralight o Mifare Classic Mini, 1K o 4K), además del tipo de tarjeta escogido por el usuario. Las tarjetas contienen sectores cuyo identificador es una combinación del número del sector junto con el nombre de la tarjeta, y puede ser autenticado por al menos una clave. Para cada sector se almacena una serie de bloques identificados a través del número de bloque combinado con el identificador del sector (nombre de la tarjeta y número de sector). Cada tarjeta (si es de transporte) puede estar relacionada con una o varias estaciones.

# CAPÍTULO 4: PRUEBAS

---

Este capítulo recoge un conjunto de pruebas necesarias para comprobar el correcto funcionamiento del sistema, además de una serie de resultados obtenidos y a comparar con los generados a través de otros medios.

## 1. Pruebas del sistema

En este apartado se describirán las pruebas para comprobar las funcionalidades del sistema implementado. Cada una de las pruebas viene acompañada de ciertos datos compactados en una tabla con el siguiente formato:

<b>Identificador</b>	PSF-XX
<b>Descripción</b>	Descripción de la prueba
<b>Pasos</b>	Pasos de la prueba
<b>Posibles errores</b>	Posibles errores de la prueba
<b>Requisitos</b>	Requisitos de la prueba
<b>Resultado esperado</b>	Resultado esperado al concluir la prueba

**Tabla 204:** Formato tabla de prueba del sistema

Cuyos campos significan:

- **Identificador:** identificador de la prueba con la estructura PSF-XX, donde XX es el número que identifica la prueba.
- **Descripción:** descripción de la prueba.
- **Pasos:** secuencia de pasos para realizar la prueba.
- **Posibles errores:** posibles errores que impidan superar la prueba.
- **Requisitos:** requisitos relacionados con la prueba.
- **Resultado esperado:** resultado que se espera conseguir al concluir la prueba para considerar que esta ha terminado adecuadamente.

### 1.1. Especificación de pruebas del sistema

<b>Identificador</b>	PSF-01
<b>Descripción</b>	Se comprobará que un usuario puede leer y almacenar una tarjeta RFID de tipo Mifare Classic Mini.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Leer”.</li> <li>3. Seleccionar las claves necesarias para la lectura.</li> <li>4. Pulsar sobre el botón “Leer”.</li> <li>5. Acercar al dispositivo la tarjeta a leer.</li> <li>6. Escribir el nombre de la tarjeta.</li> <li>7. Seleccionar un tipo de tarjeta.</li> <li>8. Si se desea, modificar el contenido de la tarjeta.</li> <li>9. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al leer un bloque.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-02, RSF-08, RSF-09, RSF-10, RSF-11, RSF-19, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es leída, almacenada y mostrada por pantalla.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 205: Prueba PSF-01 – Leer tarjeta Mifare Classic Mini**

<b>Identificador</b>	PSF-02
<b>Descripción</b>	Se comprobará que un usuario puede leer y almacenar una tarjeta RFID de tipo Mifare Classic 1K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Leer”.</li> <li>3. Seleccionar las claves necesarias para la lectura.</li> <li>4. Pulsar sobre el botón “Leer”.</li> <li>5. Acercar al dispositivo la tarjeta a leer.</li> <li>6. Escribir el nombre de la tarjeta.</li> <li>7. Seleccionar un tipo de tarjeta.</li> <li>8. Si se desea, modificar el contenido de la tarjeta.</li> <li>9. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al leer un bloque.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-03, RSF-08, RSF-09, RSF-10, RSF-11, RSF-19, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es leída, almacenada y mostrada por pantalla.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 206: Prueba PSF-02 – Leer tarjeta Mifare Classic 1K**

<b>Identificador</b>	PSF-03
<b>Descripción</b>	Se comprobará que un usuario puede leer y almacenar una tarjeta RFID de tipo Mifare Classic 4K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Leer”.</li> <li>3. Seleccionar las claves necesarias para la lectura.</li> <li>4. Pulsar sobre el botón “Leer”.</li> <li>5. Acercar al dispositivo la tarjeta a leer.</li> <li>6. Escribir el nombre de la tarjeta.</li> <li>7. Seleccionar un tipo de tarjeta.</li> <li>8. Si se desea, modificar el contenido de la tarjeta.</li> <li>9. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al leer un bloque.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-04, RSF-08, RSF-09, RSF-10, RSF-11, RSF-19, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es leída, almacenada y mostrada por pantalla.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 207: Prueba PSF-03 – Leer tarjeta Mifare Classic 4K

<b>Identificador</b>	PSF-04
<b>Descripción</b>	Se comprobará que un usuario puede leer y almacenar una tarjeta RFID de tipo Mifare Ultralight.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Leer”.</li> <li>3. No seleccionar ninguna clave para la lectura.</li> <li>4. Pulsar sobre el botón “Leer”.</li> <li>5. Acercar al dispositivo la tarjeta a leer.</li> <li>6. Escribir el nombre de la tarjeta.</li> <li>7. Seleccionar un tipo de tarjeta.</li> <li>8. Si se desea, modificar el contenido de la tarjeta.</li> <li>9. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al leer un bloque.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-01, RSF-08, RSF-11, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es leída, almacenada y mostrada por pantalla.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 208: Prueba PSF-04 – Leer tarjeta Mifare Ultralight

<b>Identificador</b>	PSF-05
<b>Descripción</b>	Se comprobará que un usuario puede escribir una tarjeta RFID de tipo Mifare Classic Mini.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Escribir”.</li> <li>3. Seleccionar la tarjeta que se quiere escribir.</li> <li>4. Seleccionar las claves necesarias para la escritura.</li> <li>5. Pulsar sobre el botón “Escribir”.</li> <li>6. Acercar al dispositivo la tarjeta a escribir.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al escribir un bloque.</li> <li>• Error al leer información de la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-13, RSF-16, RSF-17, RSF-18, RSF-19, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es escrita.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 209: Prueba PSF-05 – Escribir tarjeta Mifare Classic Mini**

<b>Identificador</b>	PSF-06
<b>Descripción</b>	Se comprobará que un usuario puede escribir una tarjeta RFID de tipo Mifare Classic 1K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Escribir”.</li> <li>3. Seleccionar la tarjeta que se quiere escribir.</li> <li>4. Seleccionar las claves necesarias para la escritura.</li> <li>5. Pulsar sobre el botón “Escribir”.</li> <li>6. Acercar al dispositivo la tarjeta a escribir.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al escribir un bloque.</li> <li>• Error al leer información de la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-14, RSF-16, RSF-17, RSF-18, RSF-19, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es escrita.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 210: Prueba PSF-06 – Escribir tarjeta Mifare Classic 1K**



<b>Identificador</b>	PSF-07
<b>Descripción</b>	Se comprobará que un usuario puede escribir una tarjeta RFID de tipo Mifare Classic 4K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Escribir”.</li> <li>3. Seleccionar la tarjeta que se quiere escribir.</li> <li>4. Seleccionar las claves necesarias para la escritura.</li> <li>5. Pulsar sobre el botón “Escribir”.</li> <li>6. Acercar al dispositivo la tarjeta a escribir.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al escribir un bloque.</li> <li>• Error al leer información de la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-15, RSF-16, RSF-17, RSF-18, RSF-19, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es escrita.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 211: Prueba PSF-07 – Escribir tarjeta Mifare Classic 4K**

<b>Identificador</b>	PSF-08
<b>Descripción</b>	Se comprobará que un usuario puede escribir una tarjeta RFID de tipo Mifare Ultralight.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Escribir”.</li> <li>3. Seleccionar la tarjeta que se quiere escribir.</li> <li>4. No seleccionar ninguna clave para la escritura.</li> <li>5. Pulsar sobre el botón “Escribir”.</li> <li>6. Acercar al dispositivo la tarjeta a escribir.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al conectar con la tarjeta.</li> <li>• Error al escribir un bloque.</li> <li>• Error al leer información de la base de datos.</li> <li>• No hay acceso a internet y no se guardan las claves en el backend.</li> </ul>
<b>Requisitos</b>	RSF-12, RSF-18, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es escrita.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 212: Prueba PSF-08 – Escribir tarjeta Mifare Ultralight**

<b>Identificador</b>	PSF-09
<b>Descripción</b>	Se comprobará que un usuario puede crear una tarjeta RFID de tipo Mifare Classic Mini.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Ver escaneados”.</li> <li>3. Pulsar sobre la opción “Crear Tag” en el menú desplegable.</li> <li>4. Pulsar sobre el tipo de Tarjeta “Mifare Classic Mini”.</li> <li>5. Escribir el nombre de la tarjeta.</li> <li>6. Seleccionar un tipo de tarjeta.</li> <li>7. Modificar el contenido de la tarjeta.</li> <li>8. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-23, RSF-26, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es creada y almacenada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 213:** Prueba PSF-09 – Crear tarjeta Mifare Classic Mini

<b>Identificador</b>	PSF-10
<b>Descripción</b>	Se comprobará que un usuario puede crear una tarjeta RFID de tipo Mifare Classic 1K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Ver escaneados”.</li> <li>3. Pulsar sobre la opción “Crear Tag” en el menú desplegable.</li> <li>4. Pulsar sobre el tipo de Tarjeta “Mifare Classic 1K”.</li> <li>5. Escribir el nombre de la tarjeta.</li> <li>6. Seleccionar un tipo de tarjeta.</li> <li>7. Modificar el contenido de la tarjeta.</li> <li>8. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-24, RSF-26, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es creada y almacenada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 214:** Prueba PSF-10 – Crear tarjeta Mifare Classic 1K

<b>Identificador</b>	PSF-11
<b>Descripción</b>	Se comprobará que un usuario puede crear una tarjeta RFID de tipo Mifare Classic 4K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Ver escaneados”.</li> <li>3. Pulsar sobre la opción “Crear Tag” en el menú desplegable.</li> <li>4. Pulsar sobre el tipo de Tarjeta “Mifare Classic 4K”.</li> <li>5. Escribir el nombre de la tarjeta.</li> <li>6. Seleccionar un tipo de tarjeta.</li> <li>7. Modificar el contenido de la tarjeta.</li> <li>8. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-25, RSF-26, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es creada y almacenada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 215: Prueba PSF-11 – Crear tarjeta Mifare Classic 4K**

<b>Identificador</b>	PSF-12
<b>Descripción</b>	Se comprobará que un usuario puede crear una tarjeta RFID de tipo Mifare Ultralight.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Ver escaneados”.</li> <li>3. Pulsar sobre la opción “Crear Tag” en el menú desplegable.</li> <li>4. Pulsar sobre el tipo de Tarjeta “Mifare Ultralight”.</li> <li>5. Escribir el nombre de la tarjeta.</li> <li>6. Seleccionar un tipo de tarjeta.</li> <li>7. Modificar el contenido de la tarjeta.</li> <li>8. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-22, RSF-26, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es creada y almacenada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 216: Prueba PSF-12 – Crear tarjeta Mifare Ultralight**

<b>Identificador</b>	PSF-13
<b>Descripción</b>	Se comprobará que un usuario puede modificar una tarjeta RFID.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Ver escaneados”.</li> <li>3. Seleccionar la tarjeta a modificar.</li> <li>4. Modificar la información deseada (nombre, tipo o contenido).</li> <li>5. Pulsar sobre el icono “Guardar” en la barra de menú.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al modificar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-20, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es modificada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 217: Prueba PSF-13 – Modificar tarjeta RFID

<b>Identificador</b>	PSF-14
<b>Descripción</b>	Se comprobará que un usuario puede borrar una tarjeta RFID.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Ver escaneados”.</li> <li>3. Mantener pulsada la tarjeta que se desea eliminar.</li> <li>4. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> <li>• Error al eliminar información de la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-21, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es eliminada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 218: Prueba PSF-14 – Borrar tarjeta RFID

<b>Identificador</b>	PSF-15
<b>Descripción</b>	Se comprobará que un usuario puede importar una tarjeta RFID de tipo Mifare Classic Mini.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con el contenido de una tarjeta Mifare Classic Mini y con el nombre “tarjetaMini_mfcMini.dmp”.</li> <li>2. Iniciar la aplicación.</li> <li>3. Pulsar sobre el botón “Ver escaneados”.</li> <li>4. Pulsar sobre la opción “Importar tags” en el menú desplegable.</li> <li>5. Introducir la dirección donde se encuentra el fichero indicado en el paso 1.</li> <li>6. Seleccionar la opción “Importar claves de tarjeta”.</li> <li>7. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer el fichero a importar.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-31, RSF-33, RSF-34, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es importada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 219: Prueba PSF-15 – Importar tarjeta Mifare Classic Mini

<b>Identificador</b>	PSF-16
<b>Descripción</b>	Se comprobará que un usuario puede importar una tarjeta RFID de tipo Mifare Classic 1K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con el contenido de una tarjeta Mifare Classic 1K y con el nombre "tarjeta1K_mfc1k.dmp".</li> <li>2. Iniciar la aplicación.</li> <li>3. Pulsar sobre el botón "Ver escaneados".</li> <li>4. Pulsar sobre la opción "Importar tags" en el menú desplegable.</li> <li>5. Introducir la dirección donde se encuentra el fichero indicado en el paso1.</li> <li>6. Seleccionar la opción "Importar claves de tarjeta".</li> <li>7. Pulsar sobre el botón "Aceptar".</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer el fichero a importar.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-31, RSF-33, RSF-34, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es importada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 220: Prueba PSF-16 – Importar tarjeta Mifare Classic 1K

<b>Identificador</b>	PSF-17
<b>Descripción</b>	Se comprobará que un usuario puede importar una tarjeta RFID de tipo Mifare Classic 4K.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con el contenido de una tarjeta Mifare Classic 4K y con el nombre "tarjeta4K_mfc4k.dmp".</li> <li>2. Iniciar la aplicación.</li> <li>3. Pulsar sobre el botón "Ver escaneados".</li> <li>4. Pulsar sobre la opción "Importar tags" en el menú desplegable.</li> <li>5. Introducir la dirección donde se encuentra el fichero indicado en el paso1.</li> <li>6. Seleccionar la opción "Importar claves de tarjeta".</li> <li>7. Pulsar sobre el botón "Aceptar".</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer el fichero a importar.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-31, RSF-33, RSF-34, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es importada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 221: Prueba PSF-17 – Importar tarjeta Mifare Classic 4K

<b>Identificador</b>	PSF-18
<b>Descripción</b>	Se comprobará que un usuario puede importar una tarjeta RFID de tipo Mifare Ultralight.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con el contenido de una tarjeta Mifare Ultralight y con el nombre "tarjeta_mfu.dmp".</li> <li>2. Iniciar la aplicación.</li> <li>3. Pulsar sobre el botón "Ver escaneados".</li> <li>4. Pulsar sobre la opción "Importar tags" en el menú desplegable.</li> <li>5. Introducir la dirección donde se encuentra el fichero indicado en el paso1.</li> <li>6. No seleccionar la opción "Importar claves de tarjeta".</li> <li>7. Pulsar sobre el botón "Aceptar".</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer el fichero a importar.</li> <li>• Dispositivo sin memoria y no se almacena la tarjeta.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-31, RSF-34, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es importada.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 222: Prueba PSF-18 – Importar tarjeta Mifare Ultralight

<b>Identificador</b>	PSF-19
<b>Descripción</b>	Se comprobará que un usuario puede importar varias tarjetas RFID de tipo Mifare (Classic o Ultralight).
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con el contenido de una tarjeta Mifare Ultralight y con el nombre "tarjeta_mfu.dmp".</li> <li>2. Guardar en el mismo directorio que en el paso1 un fichero con el contenido de una tarjeta Mifare Classic 1K y con el nombre "tarjeta1K_mfc1k.dmp".</li> <li>3. Iniciar la aplicación.</li> <li>4. Pulsar sobre el botón "Ver escaneados".</li> <li>5. Pulsar sobre la opción "Importar tags" en el menú desplegable.</li> <li>6. Introducir el directorio que contiene los ficheros indicados en el paso1.</li> <li>7. Seleccionar la opción "Importar claves de tarjeta".</li> <li>8. Pulsar sobre el botón "Aceptar".</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer los ficheros a importar.</li> <li>• Dispositivo sin memoria y no se almacenan las tarjetas.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-32, RSF-33, RSF-34, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Las tarjetas son importadas.</li> <li>• En pantalla se muestra la lista con las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 223: Prueba PSF-19 – Importar varias tarjetas Mifare

<b>Identificador</b>	PSF-20
<b>Descripción</b>	Se comprobará que un usuario puede crear una clave.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Pulsar sobre el icono “Nuevas claves” en la barra de menú.</li> <li>4. Escribir una clave hexadecimal de 12 dígitos.</li> <li>5. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la clave.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-36, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La clave es guardada.</li> <li>• En pantalla se muestra la lista con las claves almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 224: Prueba PSF-20 – Crear clave**

<b>Identificador</b>	PSF-21
<b>Descripción</b>	Se comprobará que un usuario puede crear varias claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Pulsar sobre el icono “Nuevas claves” en la barra de menú.</li> <li>4. Escribir varias claves hexadecimales de 12 dígitos cada una en una línea.</li> <li>5. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacenan las claves.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-37, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Las claves son guardadas.</li> <li>• En pantalla se muestra la lista con las claves almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 225: Prueba PSF-21 – Crear varias claves**

<b>Identificador</b>	PSF-22
<b>Descripción</b>	Se comprobará que un usuario puede modificar una clave.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Pulsar sobre la clave a modificar.</li> <li>4. Modificar la clave.</li> <li>5. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena la clave.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al modificar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-38, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La clave es modificada.</li> <li>• En pantalla se muestra la lista con las claves almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 226: Prueba PSF-22 – Modificar clave**

<b>Identificador</b>	PSF-23
<b>Descripción</b>	Se comprobará que un usuario puede eliminar una clave.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Mantener pulsada la clave a eliminar.</li> <li>4. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> <li>• Error al eliminar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-39, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La clave es eliminada.</li> <li>• En pantalla se muestra la lista con las claves almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 227: Prueba PSF-23 – Eliminar clave**

<b>Identificador</b>	PSF-24
<b>Descripción</b>	Se comprobará que un usuario puede crear un grupo de claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Pulsar sobre la opción “Crear grupo de claves” en el menú desplegable.</li> <li>4. Escribir el nombre del grupo de claves.</li> <li>5. Seleccionar las claves que componen el grupo de claves.</li> <li>6. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena el grupo de claves.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-40, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El grupo de claves es almacenado.</li> <li>• En pantalla se muestra la lista de grupos de claves almacenados.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 228: Prueba PSF-24 – Crear grupo de claves**

<b>Identificador</b>	PSF-25
<b>Descripción</b>	Se comprobará que un usuario puede modificar un grupo de claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Cambiar a la ventana de los grupos de claves.</li> <li>4. Pulsar sobre el grupo de claves a modificar.</li> <li>5. Pulsar sobre icono “Editar” en la barra superior.</li> <li>6. Modificar la información deseada (Nombre del grupo o claves).</li> <li>7. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacena el grupo de claves.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al modificar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-41, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El grupo de claves es modificado.</li> <li>• En pantalla se muestra la lista de grupos de claves almacenados.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 229: Prueba PSF-25 – Modificar grupo de claves**



<b>Identificador</b>	PSF-26
<b>Descripción</b>	Se comprobará que un usuario puede eliminar un grupo de claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Claves”.</li> <li>3. Cambiar a la ventana de los grupos de claves.</li> <li>4. Mantener pulsado el grupo de claves a eliminar.</li> <li>5. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> <li>• Error al eliminar información de la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-42, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El grupo de claves es eliminado.</li> <li>• En pantalla se muestra la lista de grupos de claves almacenados.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 230:** Prueba PSF-26 – Eliminar grupo de claves

<b>Identificador</b>	PSF-27
<b>Descripción</b>	Se comprobará que un usuario puede importar un fichero de claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con las claves a importar (una clave por línea) y cuya extensión sea “.txt”.</li> <li>2. Iniciar la aplicación.</li> <li>3. Pulsar sobre el botón “Claves”.</li> <li>4. Pulsar sobre la opción “Importar claves” en el menú desplegable.</li> <li>5. Introducir la dirección donde se encuentra el fichero indicado en el paso1.</li> <li>6. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer el fichero a importar.</li> <li>• Dispositivo sin memoria y no se almacenan las claves.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-43, RSF-45, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Las claves son importadas.</li> <li>• En pantalla se muestra la lista de claves almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 231:** Prueba PSF-27 – Importar un fichero de claves

<b>Identificador</b>	PSF-28
<b>Descripción</b>	Se comprobará que un usuario puede importar varios ficheros de claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Guardar en el dispositivo un fichero con las claves a importar (una clave por línea) y cuya extensión sea “.txt”.</li> <li>2. Guardar otro fichero con otras claves a importar (una clave por línea) y cuya extensión sea “.txt”.</li> <li>3. Iniciar la aplicación.</li> <li>4. Pulsar sobre el botón “Claves”.</li> <li>5. Pulsar sobre la opción “Importar claves” en el menú desplegable.</li> <li>6. Introducir el directorio que contiene los ficheros indicados en el paso1.</li> <li>7. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer el fichero a importar.</li> <li>• Dispositivo sin memoria y no se almacenan las claves.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-44, RSF-45, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Las claves son importadas.</li> <li>• En pantalla se muestra la lista de claves almacenadas.</li> <li>• Aparece un mensaje indicando que la operación ha terminado correctamente.</li> </ul>

Tabla 232: Prueba PSF-28 – Importar varios ficheros de claves

<b>Identificador</b>	PSF-29
<b>Descripción</b>	Se comprobará que un usuario puede crear nuevos tipos de tarjetas RFID.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> <li>2. Escoger la opción “--Nuevo tipo--” en el tipo de tarjeta.</li> <li>3. Escribir el nuevo tipo.</li> <li>4. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacenan las claves.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-05, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El tipo de tarjeta es almacenado.</li> <li>• En la lista de tipos de tarjetas se puede seleccionar el nuevo tipo.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 233: Prueba PSF-29 – Crear tipo de tarjeta

<b>Identificador</b>	PSF-30
<b>Descripción</b>	Se comprobará que un usuario puede renombrar una tarjeta RFID.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> <li>2. Escribir el nombre de una tarjeta que ya exista en la base de datos.</li> <li>3. Pulsar sobre el icono “Guardar” en la barra de menú.</li> <li>4. Pulsar sobre el botón “Renombrar”.</li> <li>5. Introducir el nuevo nombre de la tarjeta.</li> <li>6. Pulsar sobre el botón “Aceptar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacenan las claves.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-06, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es almacenada con el nuevo nombre.</li> <li>• En pantalla se muestra la lista de las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

Tabla 234: Prueba PSF-30 – Renombrar tarjeta RFID

<b>Identificador</b>	PSF-31
<b>Descripción</b>	Se comprobará que un usuario puede reemplazar una tarjeta RFID.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> <li>2. Escribir el nombre de una tarjeta que ya exista en la base de datos.</li> <li>3. Pulsar sobre el icono “Guardar” en la barra de menú.</li> <li>4. Pulsar sobre el botón “Reemplazar”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Dispositivo sin memoria y no se almacenan las claves.</li> <li>• Error al leer información de la base de datos.</li> <li>• Error al insertar información en la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-07, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• La tarjeta es almacenada sustituyendo a la anterior.</li> <li>• En pantalla se muestra la lista de las tarjetas almacenadas.</li> <li>• Aparece un mensaje temporal indicando que la operación se ha llevado a cabo correctamente.</li> </ul>

**Tabla 235: Prueba PSF-31 – Reemplazar tarjeta RFID**

<b>Identificador</b>	PSF-32
<b>Descripción</b>	Se comprobará que un usuario puede ver una tarjeta RFID en formato ASCII.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> <li>2. Pulsar sobre la opción “Ver como ASCII” en el menú desplegable.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-27, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El contenido de la tarjeta será mostrado en formato ASCII.</li> </ul>

**Tabla 236: Prueba PSF-32 – Ver tarjeta RFID en formato ASCII**

<b>Identificador</b>	PSF-33
<b>Descripción</b>	Se comprobará que un usuario puede ver una tarjeta RFID en formato hexadecimal.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> </ul>
<b>Requisitos</b>	RSF-28, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El contenido de la tarjeta será mostrado en formato hexadecimal.</li> </ul>

**Tabla 237: Prueba PSF-33 – Ver tarjeta RFID en formato hexadecimal**

<b>Identificador</b>	PSF-34
<b>Descripción</b>	Se comprobará que un usuario puede ver una tarjeta RFID como tarjeta de transporte.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> <li>2. Pulsar sobre la opción “Ver como tarjeta de transporte” en el menú desplegable.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> <li>• Información de tarjeta errónea al convertirla en tarjeta de transporte.</li> </ul>
<b>Requisitos</b>	RSF-29, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• El contenido de la tarjeta será mostrado como tarjeta de transporte.</li> </ul>

**Tabla 238: Prueba PSF-34 – Ver tarjeta RFID como tarjeta de transporte**

<b>Identificador</b>	PSF-35
<b>Descripción</b>	Se comprobará que un usuario puede ver las condiciones de acceso de una tarjeta RFID.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Leer (PSF-01/02/03/04) o modificar (PSF-13) tarjeta RFID.</li> <li>2. Pulsar sobre la opción “Ver condiciones de acceso” en el menú desplegable.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• Error al leer información de la base de datos.</li> <li>• Error al decodificar las condiciones de acceso de la tarjeta.</li> </ul>
<b>Requisitos</b>	RSF-30, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Las condiciones de acceso serán mostradas.</li> </ul>

**Tabla 239: Prueba PSF-35 – Ver condiciones de acceso de una tarjeta RFID**

<b>Identificador</b>	PSF-36
<b>Descripción</b>	Se comprobará que un usuario puede ver las estadísticas de uso de las claves.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Iniciar la aplicación.</li> <li>2. Pulsar sobre el botón “Estadísticas”.</li> </ol>
<b>Posibles errores</b>	<ul style="list-style-type: none"> <li>• No hay acceso a internet y no se obtienen las claves del backend.</li> </ul>
<b>Requisitos</b>	RSF-35, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Tabla con el número de lecturas, escrituras y el porcentaje de ambos valores de una clave sobre el total de todas las claves.</li> </ul>

**Tabla 240: Prueba PSF-36 – Ver estadísticas de uso de las claves**

<b>Identificador</b>	PSF-37
<b>Descripción</b>	Se comprobará que un usuario puede activar la tecnología NFC a través de la aplicación.
<b>Pasos</b>	<ol style="list-style-type: none"> <li>1. Desactivar tecnología NFC.</li> <li>2. Iniciar la aplicación.</li> <li>3. Pulsar sobre el botón “Ajustes” en el diálogo “NFC desactivado”.</li> <li>4. Activar la tecnología NFC.</li> </ol>
<b>Posibles errores</b>	
<b>Requisitos</b>	RSF-46, RSF-47, RSF-48, RSF-49
<b>Resultado esperado</b>	<ul style="list-style-type: none"> <li>• Activada tecnología NFC del dispositivo.</li> </ul>

**Tabla 241: Prueba PSF-37 – Activación tecnología NFC**

## 1.2. Trazabilidad entre requisitos software funcionales y pruebas del sistema

En esta sección se va a mostrar la relación existente entre cada requisito software funcional y las pruebas del sistema.

	RSF-01	RSF-02	RSF-03	RSF-04	RSF-05	RSF-06	RSF-07	RSF-08	RSF-09	RSF-10	RSF-11	RSF-12	RSF-13	RSF-14	RSF-15	RSF-16	RSF-17	RSF-18	RSF-19	RSF-20	RSF-21	RSF-22	RSF-23	RSF-24	RSF-25	RSF-26	RSF-27	RSF-28	RSF-29	RSF-30	RSF-31	RSF-32	RSF-33	RSF-34	RSF-35	RSF-36	RSF-37	RSF-38	RSF-39	RSF-40	RSF-41	RSF-42	RSF-43	RSF-44	RSF-45	RSF-46	RSF-47	RSF-48	RSF-49
PSF-01	X						X	X	X	X									X																											X	X	X	
PSF-02		X					X	X	X	X									X																											X	X	X	
PSF-03			X				X	X	X	X									X																											X	X	X	
PSF-04	X						X			X																																					X	X	X
PSF-05													X			X	X	X	X																											X	X	X	
PSF-06														X		X	X	X	X																											X	X	X	
PSF-07															X	X	X	X	X																											X	X	X	
PSF-08											X							X																													X	X	X
PSF-09																							X				X																				X	X	X
PSF-10																								X		X																					X	X	X
PSF-11																									X	X																					X	X	X
PSF-12																						X				X																					X	X	X
PSF-13																				X																											X	X	X
PSF-14																					X																										X	X	X
PSF-15																																	X		X	X											X	X	X
PSF-16																																	X		X	X										X	X	X	
PSF-17																																	X		X	X										X	X	X	
PSF-18																																	X		X											X	X	X	
PSF-19																																		X	X	X										X	X	X	
PSF-20																																				X											X	X	X
PSF-21																																					X										X	X	X
PSF-22																																						X									X	X	X

[illegible]

**Tabla 242:** Matriz de trazabilidad entre requisitos software funcionales y pruebas del sistema

## 2. Resultados

Además de las pruebas del sistema se han realizado una serie de comparaciones para comprobar que los resultados obtenidos con la aplicación son correctos. Para ello se utiliza un lector de tarjetas RFID junto con las librerías LibNFC o el programa Mfoc. El resultado de esta operación es almacenado en un fichero en formato hexadecimal y cargado en una página web para decodificarlo a formato legible [56] . En las tarjetas de transporte también se utiliza el programa Mfoc GUI para decodificar la información de transporte leída.

Para poder leer las tarjetas RFID de tipo Mifare Classic a través del dispositivo móvil es necesario conocer sus claves de autenticación, las cuales son obtenidas a través de la Proxmark3. Debido a que el proceso de obtención de claves requiere mucho tiempo y que es idéntico para el resto de pruebas solamente se mostrará este resultado para la primera tarjeta Mifare Classic 1K.

### 2.1. Prueba 1 – Lectura tarjeta Mifare Ultralight

En esta prueba se lee una tarjeta RFID de tipo Mifare Ultralight a través del dispositivo móvil y utilizando un lector de tarjetas en conjunto con las librerías LibNFC.

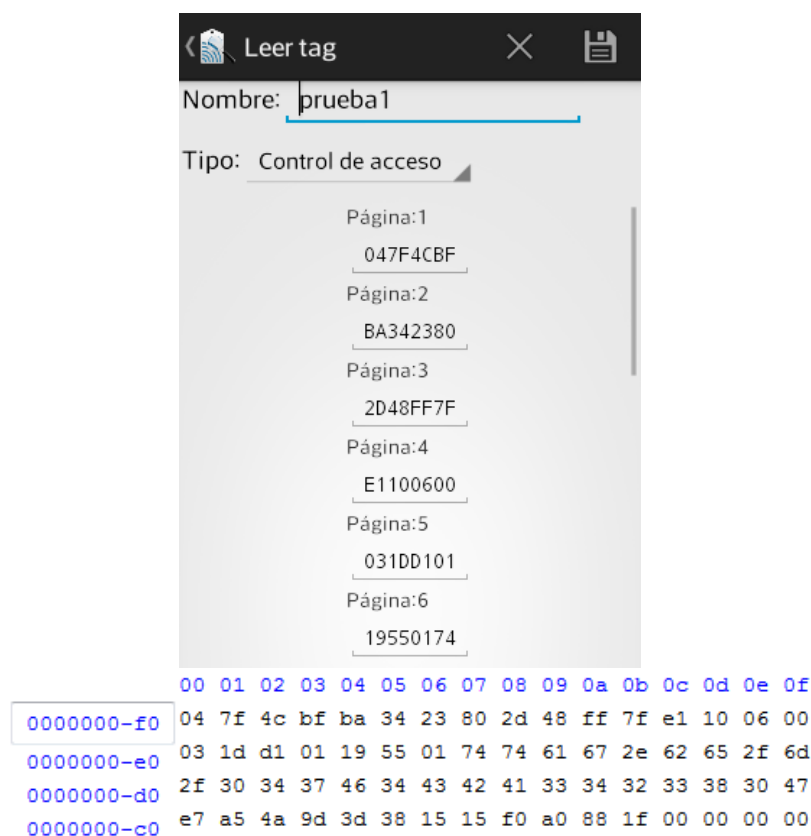


Ilustración 19: Prueba 1 – Resultado de dispositivo móvil (arriba) y del lector con LibNFC (abajo)

En esta primera prueba se puede observar que la información leída por el dispositivo es idéntica a la obtenida por el lector, por lo tanto la lectura de tarjetas RFID de tipo Mifare Ultralight es correcta.

## 2.2. Prueba 2 – Lectura tarjeta Mifare Classic 1K

En esta prueba se lee una tarjeta RFID de tipo Mifare Classic 1K a través del dispositivo móvil y el lector de tarjetas junto con el programa Mfoc. En esta prueba la tarjeta posee diferentes claves de autenticación en los sectores.

The image displays two screenshots related to the Mifare Classic 1K key extraction process.

**Top Screenshot (Proxmark3 Terminal):** Shows the output of a key extraction attempt. It indicates a valid key was found: 45fa8e28c55a, with 56 iterations. Below this, a table lists the extracted keys for sectors 000 to 015. The table has columns for 'sec', 'key A', 'res', 'key B', and 'res'. The 'res' column contains the value '1' for all sectors. The keys are listed in hexadecimal. At the bottom, it says 'Printing keys to binary file dumpkeys.bin...' and 'proxmark3> proxmark3>'.

sec	key A	res	key B	res
000	a0a1a2a3a4a5	1	08d4bdeed155	1
001	a0a1a2a3a4a5	1	1dfb912e38d5	1
002	4231ed70f7cf	1	f7bf1e67470e	1
003	11e7285c4a99	1	833831d55f56	1
004	3cf740c5c972	1	f96b97accbd2	1
005	185643eb1e28	1	b637cc9f5e0c	1
006	966f3c49e14a	1	26417c6ce88a	1
007	f291b1b3f1bb	1	9a3f838852ef	1
008	b4882b71be01	1	7239ff074a33	1
009	c30d6c6f139c	1	3899face60bb	1
010	5e9d1862e1ad	1	c9551ba7f352	1
011	4582db3f91e3	1	b7fce7cf69e0	1
012	7b2c5b9b2492	1	31327fba6490	1
013	3795841e8964	1	45fa8e28c55a	1
014	b4253eb5beaa	1	8f4c7e4933ea	1
015	421dee572fe5	1	53730e705ac3	1

**Bottom Screenshot (Mifare Classic 1K Tag Reader):** Shows the interface for reading a tag. The 'Nombre' field is filled with 'prueba2'. The 'Tipo' is set to 'Control de acceso'. The 'Sector:1' section shows the key 3C18A8B73B880400468E86584D704107. The 'Sector:2' section shows the key 920573078FFFFFFF323150460000. The 'Sector:3' section shows the key 96D4DE36030114123123590A02016203. The 'Sector:4' section shows the key 00000000000000000000000000000000. The 'Leer tag' button is visible.

Ilustración 20: Prueba 2 – Claves obtenidas a través de la Proxmark3 (arriba), resultado de dispositivo móvil (izquierda) y del lector con Mfoc (derecha)



En ambos resultados se puede observar que la información leída es idéntica y por lo tanto la lectura de tarjetas Mifare Classic 1K y la obtención de claves de autenticación es válida.

### 2.3. Prueba 3 – Lectura tarjeta Mifare Classic 1K

En esta prueba se lee una tarjeta RFID de tipo Mifare Classic 1K a través de dos medios: el dispositivo móvil y el lector de tarjetas con el programa Mfoc. La tarjeta a leer posee la clave de autenticación FFFFFFFF en todos los sectores.

The image shows two side-by-side representations of the same data. On the left is a screenshot of a mobile application titled 'Leer tag'. It displays the following information:

- Nombre: prueba3
- Tipo: Control de acceso
- Sector: 1
  - 737CA4DD7688040047BA141551300910
  - 00000000000000000000000000000000
  - 00000000000000000000000000000000
  - FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
- Sector: 2
  - 00000000000000000000000000000000
  - 00000000000000000000000000000000
  - 00000000000000000000000000000000
  - FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
- Sector: 3
  - 00000000000000000000000000000000
  - 00000000000000000000000000000000
  - 00000000000000000000000000000000
  - FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
- Sector: 4

On the right is a hex dump of the same data, showing the raw bytes in hexadecimal and ASCII format. The first row of the hex dump is highlighted in red and matches the first line of the mobile app's output.

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
0000000000	73	7c	a4	dd	76	88	04	00	47	ba	14	15	51	30	09	10
0000000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000030	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
0000000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000070	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
0000000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000b0	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
00000000c0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000d0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000f0	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
0000000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Ilustración 21: Prueba 3 – Resultado de dispositivo móvil (izquierda) y del lector con Mfoc (derecha)

Al igual que en la prueba anterior ambos resultados son idénticos.

### 2.4. Prueba 4 – Lectura tarjeta Mifare Classic 4K (tarjeta de transporte)

En esta prueba se lee una tarjeta RFID de tipo Mifare Classic 4K a través del dispositivo móvil y el lector de tarjetas junto con el programa Mfoc. Esta tarjeta es de transporte por lo que se comprobará que la lectura y la decodificación de la información de transporte son correctamente procesadas.

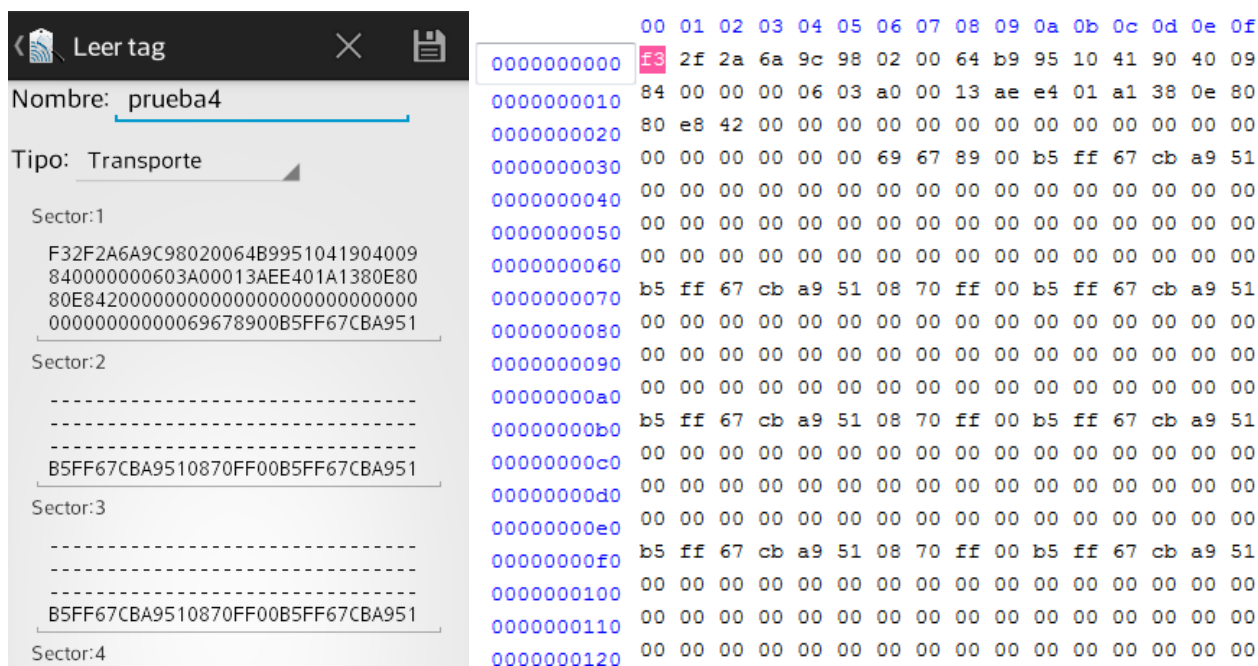


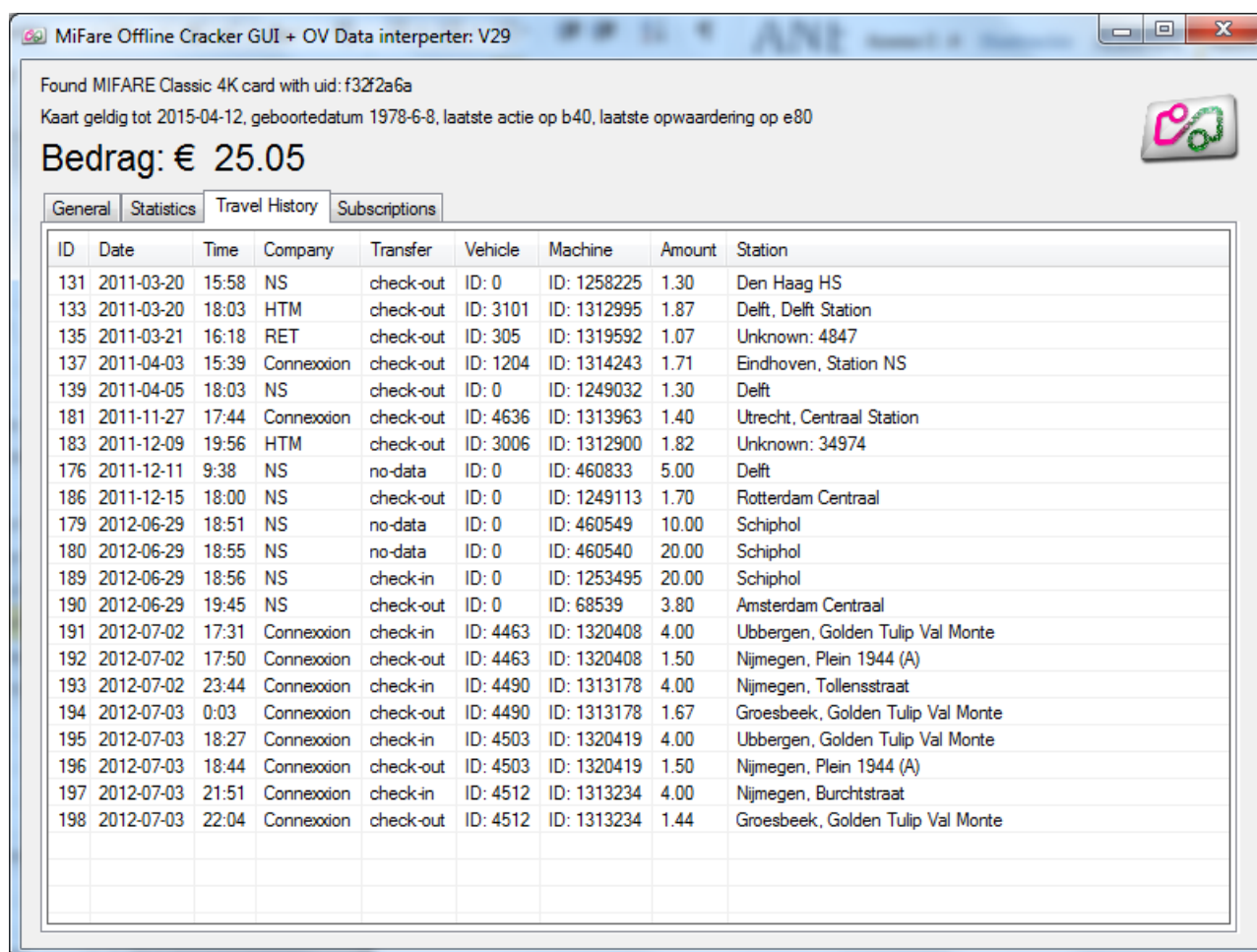
Ilustración 22: Prueba 4 – Resultado lectura de dispositivo móvil (izquierda) y del lector con Mfoc (derecha)

En ambos resultados la información leída es idéntica. A continuación se comprobará si la decodificación de la información de transporte es correcta.

### Información general



Ilustración 23: Prueba 4 – Decodificación información general de transporte con el dispositivo móvil



Found MIFARE Classic 4K card with uid: f32f2a6a  
 Kaart geldig tot 2015-04-12, geboortedatum 1978-6-8, laatste actie op b40, laatste opwaardering op e80

**Bedrag: € 25.05**

General Statistics Travel History Subscriptions

ID	Date	Time	Company	Transfer	Vehicle	Machine	Amount	Station
131	2011-03-20	15:58	NS	check-out	ID: 0	ID: 1258225	1.30	Den Haag HS
133	2011-03-20	18:03	HTM	check-out	ID: 3101	ID: 1312995	1.87	Delft, Delft Station
135	2011-03-21	16:18	RET	check-out	ID: 305	ID: 1319592	1.07	Unknown: 4847
137	2011-04-03	15:39	Connexion	check-out	ID: 1204	ID: 1314243	1.71	Eindhoven, Station NS
139	2011-04-05	18:03	NS	check-out	ID: 0	ID: 1249032	1.30	Delft
181	2011-11-27	17:44	Connexion	check-out	ID: 4636	ID: 1313963	1.40	Utrecht, Centraal Station
183	2011-12-09	19:56	HTM	check-out	ID: 3006	ID: 1312900	1.82	Unknown: 34974
176	2011-12-11	9:38	NS	no-data	ID: 0	ID: 460833	5.00	Delft
186	2011-12-15	18:00	NS	check-out	ID: 0	ID: 1249113	1.70	Rotterdam Centraal
179	2012-06-29	18:51	NS	no-data	ID: 0	ID: 460549	10.00	Schiphol
180	2012-06-29	18:55	NS	no-data	ID: 0	ID: 460540	20.00	Schiphol
189	2012-06-29	18:56	NS	check-in	ID: 0	ID: 1253495	20.00	Schiphol
190	2012-06-29	19:45	NS	check-out	ID: 0	ID: 68539	3.80	Amsterdam Centraal
191	2012-07-02	17:31	Connexion	check-in	ID: 4463	ID: 1320408	4.00	Ubbergen, Golden Tulip Val Monte
192	2012-07-02	17:50	Connexion	check-out	ID: 4463	ID: 1320408	1.50	Nijmegen, Plein 1944 (A)
193	2012-07-02	23:44	Connexion	check-in	ID: 4490	ID: 1313178	4.00	Nijmegen, Tollensstraat
194	2012-07-03	0:03	Connexion	check-out	ID: 4490	ID: 1313178	1.67	Groesbeek, Golden Tulip Val Monte
195	2012-07-03	18:27	Connexion	check-in	ID: 4503	ID: 1320419	4.00	Ubbergen, Golden Tulip Val Monte
196	2012-07-03	18:44	Connexion	check-out	ID: 4503	ID: 1320419	1.50	Nijmegen, Plein 1944 (A)
197	2012-07-03	21:51	Connexion	check-in	ID: 4512	ID: 1313234	4.00	Nijmegen, Burchtstraat
198	2012-07-03	22:04	Connexion	check-out	ID: 4512	ID: 1313234	1.44	Groesbeek, Golden Tulip Val Monte

Ilustración 24: Prueba 4 – Decodificación información general de transporte con el lector y Mfoc GUI

Se puede observar que la información decodificada en la Ilustración 23: coincide con la mostrada en la sección superior de la Ilustración 24: .

### Historial de viajes

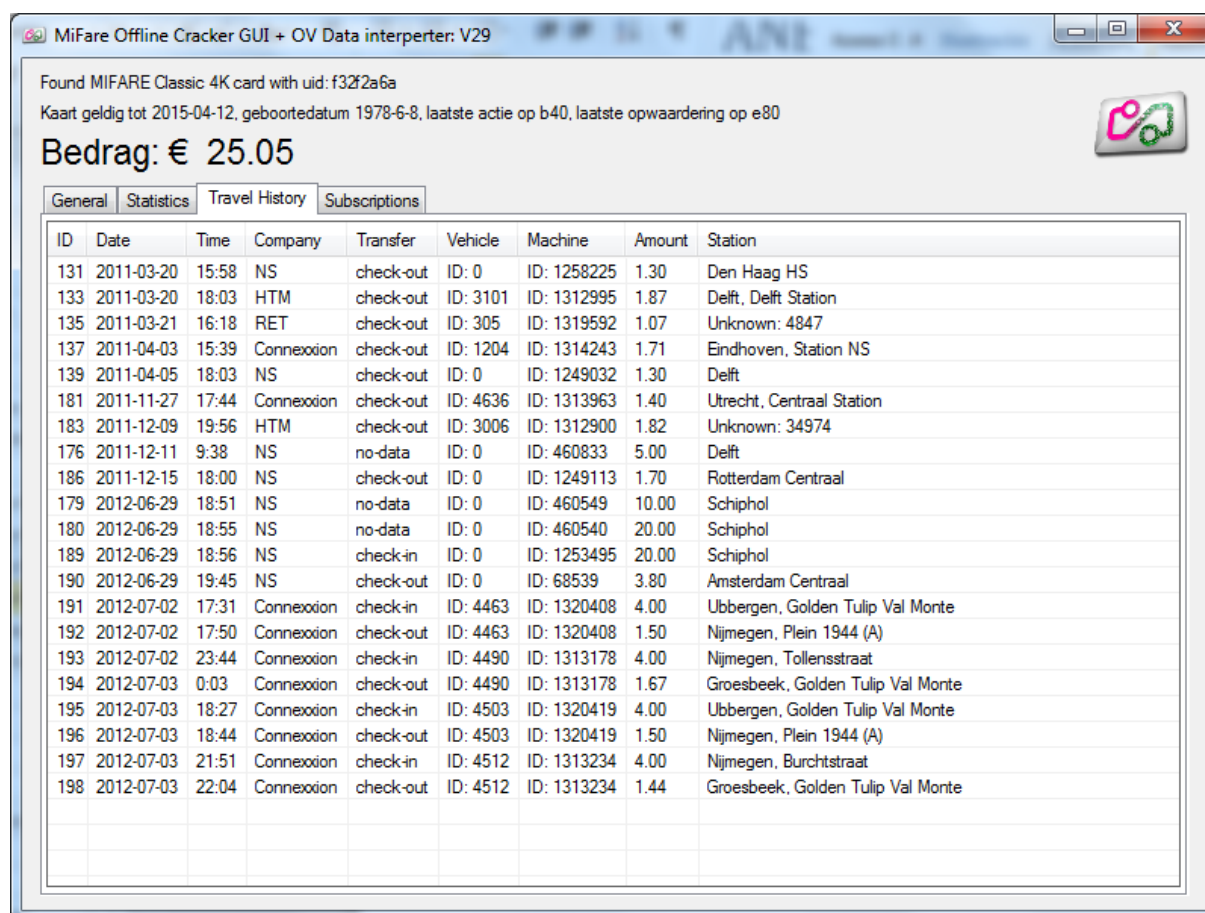


Tarjeta de transporte

GENERAL HISTORIAL DE VIAJE SUBSCRIPCIONES

ID	Fecha	Hora	Compañía	Transferencia	Vehículo	Máquina	Imp
131	2011-03-20	15:58	NS	check-out	ID: 0	ID: 1258225	1.3
133	2011-03-20	18:03	HTM	check-out	ID: 3101	ID: 1312995	1.8
135	2011-03-21	16:18	RET	check-out	ID: 305	ID: 1319592	1.0
137	2011-04-03	15:39	Connexion	check-out	ID: 1204	ID: 1314243	1.7
139	2011-04-05	18:03	NS	check-out	ID: 0	ID: 1249032	1.3
181	2011-11-27	17:44	Connexion	check-out	ID: 4636	ID: 1313963	1.4
183	2011-12-09	19:56	HTM	check-out	ID: 3006	ID: 1312900	1.8
176	2011-12-11	9:38	NS	no-data	ID: 0	ID: 460833	5.0

Ilustración 25: Prueba 4 – Decodificación historial de viajes de transporte con el dispositivo móvil



Found MIFARE Classic 4K card with uid: f32f2a6a  
Kaart geldig tot 2015-04-12, geboortedatum 1978-6-8, laatste actie op b40, laatste opwaardering op e80

**Bedrag: € 25.05**

General | Statistics | Travel History | Subscriptions

ID	Date	Time	Company	Transfer	Vehicle	Machine	Amount	Station
131	2011-03-20	15:58	NS	check-out	ID: 0	ID: 1258225	1.30	Den Haag HS
133	2011-03-20	18:03	HTM	check-out	ID: 3101	ID: 1312995	1.87	Delft, Delft Station
135	2011-03-21	16:18	RET	check-out	ID: 305	ID: 1319592	1.07	Unknown: 4847
137	2011-04-03	15:39	Connexion	check-out	ID: 1204	ID: 1314243	1.71	Eindhoven, Station NS
139	2011-04-05	18:03	NS	check-out	ID: 0	ID: 1249032	1.30	Delft
181	2011-11-27	17:44	Connexion	check-out	ID: 4636	ID: 1313963	1.40	Utrecht, Centraal Station
183	2011-12-09	19:56	HTM	check-out	ID: 3006	ID: 1312900	1.82	Unknown: 34974
176	2011-12-11	9:38	NS	no-data	ID: 0	ID: 460833	5.00	Delft
186	2011-12-15	18:00	NS	check-out	ID: 0	ID: 1249113	1.70	Rotterdam Centraal
179	2012-06-29	18:51	NS	no-data	ID: 0	ID: 460549	10.00	Schiphol
180	2012-06-29	18:55	NS	no-data	ID: 0	ID: 460540	20.00	Schiphol
189	2012-06-29	18:56	NS	check-in	ID: 0	ID: 1253495	20.00	Schiphol
190	2012-06-29	19:45	NS	check-out	ID: 0	ID: 68539	3.80	Amsterdam Centraal
191	2012-07-02	17:31	Connexion	check-in	ID: 4463	ID: 1320408	4.00	Ubbergen, Golden Tulip Val Monte
192	2012-07-02	17:50	Connexion	check-out	ID: 4463	ID: 1320408	1.50	Nijmegen, Plein 1944 (A)
193	2012-07-02	23:44	Connexion	check-in	ID: 4490	ID: 1313178	4.00	Nijmegen, Tollensstraat
194	2012-07-03	0:03	Connexion	check-out	ID: 4490	ID: 1313178	1.67	Groesbeek, Golden Tulip Val Monte
195	2012-07-03	18:27	Connexion	check-in	ID: 4503	ID: 1320419	4.00	Ubbergen, Golden Tulip Val Monte
196	2012-07-03	18:44	Connexion	check-out	ID: 4503	ID: 1320419	1.50	Nijmegen, Plein 1944 (A)
197	2012-07-03	21:51	Connexion	check-in	ID: 4512	ID: 1313234	4.00	Nijmegen, Burchtstraat
198	2012-07-03	22:04	Connexion	check-out	ID: 4512	ID: 1313234	1.44	Groesbeek, Golden Tulip Val Monte

Ilustración 26: Prueba 4 – Decodificación historial de viajes de transporte con el lector y Mfoc GUI

Cada campo del historial de viajes es decodificado correctamente pudiendo observar la información de cada estación en la que el usuario ha utilizado esta tarjeta.

### Subscripciones

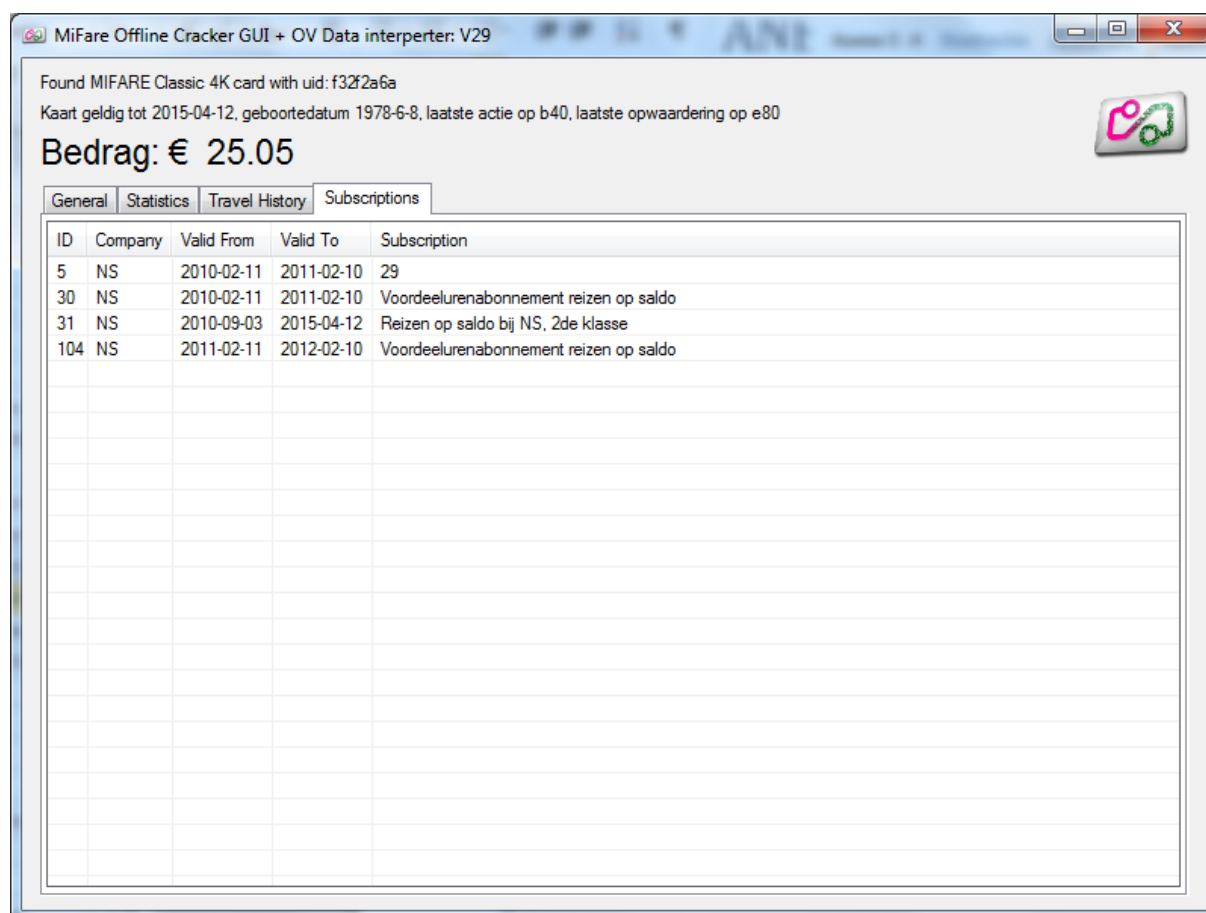


Tarjeta de transporte

HISTORIAL DE VIAJE SUBSCRIPCIONES

ID	Compañía	Válido desde	Válido hasta	Subscripción
5	NS	2010-02-11	2011-02-10	29
30	NS	2010-02-11	2011-02-10	Voordeelurenabonnement reizen c
31	NS	2010-09-03	2015-04-12	Reizen op saldo bij NS, 2de klasse
104	NS	2011-02-11	2012-02-10	Voordeelurenabonnement reizen c

Ilustración 27: Prueba 4 – Decodificación subscripciones de transporte con el dispositivo móvil



**Ilustración 28: Prueba 4 – Decodificación suscripciones de transporte con el lector y Mfoc GUI**

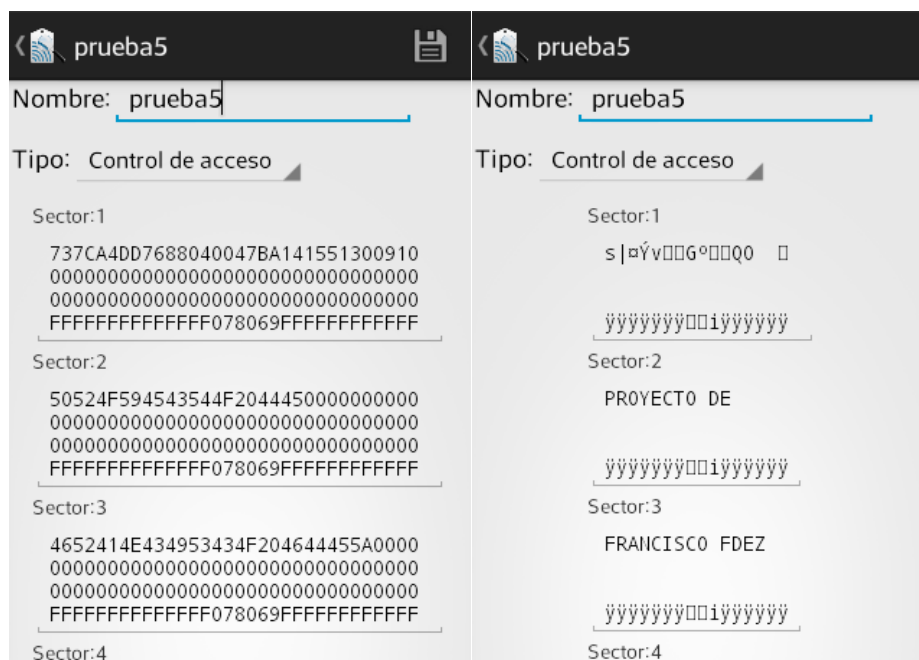
Al igual que en la decodificación anterior cada campo de las suscripciones es decodificado correctamente pudiendo observar todas las suscripciones a las que el usuario ha estado inscrito con esta tarjeta.

## 2.5. Prueba 5 – Escritura en tarjeta Mifare Classic 1K

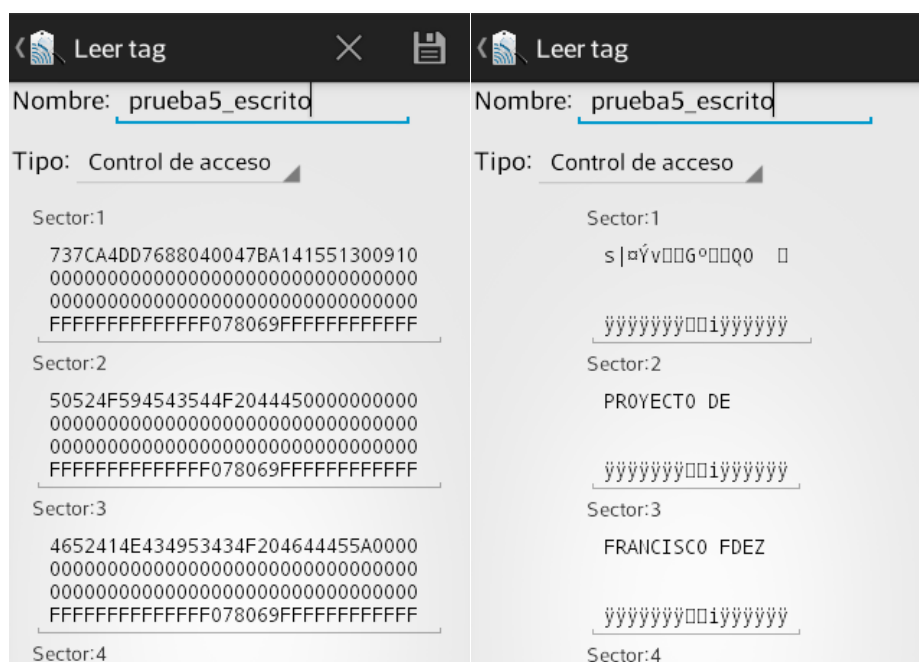
En esta prueba se escribe información en una tarjeta RFID de tipo Mifare Classic 1K a través del dispositivo móvil y posteriormente la lectura de esa misma tarjeta para comprobar que la escritura se ha llevado a cabo correctamente.

La tarjeta sobre la que se va a realizar la escritura posee la misma clave de autenticación (FFFFFFFFFFFF) en todos los sectores.

La información a escribir es “PROYECTO DE” en el primer bloque del sector 2, y “FRANCISCO FDEZ” en el primer bloque del sector 3, que en formato hexadecimal corresponde a “50524F594543544F204445” y “4652414E434953434F204644455A” respectivamente.



**Ilustración 29: Prueba 5 – Resultado modificación de tarjeta almacenada en el dispositivo móvil: hexadecimal (izquierda), ASCII (derecha)**



**Ilustración 30: Prueba 5 – Resultado lectura de dispositivo móvil de tarjeta modificada: hexadecimal (izquierda), ASCII (derecha)**

Una vez modificada la información, escrita y leída de nuevo de la tarjeta se puede observar que la operación se ha llevado correctamente. A continuación se comprobará si el resultado es correcto a través del lector y el programa Mfoc.

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
0000000000	73	7c	a4	dd	76	88	04	00	47	ba	14	15	51	30	09	10
0000000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000030	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
0000000040	50	52	4f	59	45	43	54	4f	20	44	45	00	00	00	00	00
0000000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000070	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
0000000080	46	52	41	4e	43	49	53	43	4f	20	46	44	45	5a	00	00
0000000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000b0	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
00000000c0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000d0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000f0	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff
0000000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Ilustración 31: Prueba 5 – Resultado lectura con el lector y Mfoc de una tarjeta escrita

Con esta comprobación se observa que la lectura a través del dispositivo y del lector son equivalentes, por lo que esta prueba es correcta.



# CAPÍTULO 5: CONCLUSIONES Y FUTURAS LÍNEAS DE TRABAJO

---



En este capítulo se incluyen las conclusiones obtenidas sobre el desarrollo de este proyecto y las posibles futuras líneas de trabajo que es posible aplicar sobre la aplicación para su mejora.

## 1. Conclusiones

Este proyecto ha permitido adquirir gran cantidad de conocimientos sobre el desarrollo de aplicaciones para dispositivos Android y la tecnología NFC, completamente desconocidos como desarrollador de aplicaciones para otros usuarios.

En el apartado Objetivos del primer capítulo se especificaron una serie de subobjetivos necesarios para poder alcanzar el objetivo principal de este proyecto, una aplicación Android encargada de leer, escribir, almacenar y retransmitir tarjetas RFID.

El primer objetivo planteado consistía en entender y comprender a fondo los conceptos que se van a utilizar (NFC y librerías, Proxmark3, Android y GAE). Debido a que inicialmente no se poseía ningún tipo de conocimiento ha sido necesario dedicarle un gran esfuerzo visitando foros, transparencias, artículos de investigación y webs oficiales sobre estas tecnologías para asimilar correctamente toda la información y utilizarla en posteriores tareas.

El segundo objetivo consistía en descubrir las capacidades y limitaciones de las librerías NFC. Las librerías fueron LibNFC [26] y RFIDIOt [27], ambas probadas en una máquina virtual con sistema operativo Linux. Esta conclusión no fue fácil ya que para ello fue necesario instalar dichas librerías y comprobar las capacidades de cada una de ellas, lo que conllevó las dificultades explicadas a continuación.

Inicialmente se probó la librería RFIDIOt, la cual requiere instalar una gran cantidad de paquetes para poder utilizarla, y algunos de ellos están obsoletos o no son compatibles con otros programas. Además esta librería no está documentada por lo que fue necesario analizar y comprender su código, el cual está desarrollado en Python, lenguaje que ha sido necesario aprender ya que no se tenían conocimientos previos. Esta librería fue descartada debido a que no era compatible con el lector de tarjetas Touchatag.

La librería LibNFC ocasionó algún problema para su instalación debido a que necesita unos paquetes con unas versiones muy concretas pero aun así fue mucho más fácil de probar que la librería RFIDIOt. Esta librería tampoco está documentada por lo que fue necesario el análisis de su código fuente, más sencillo que RFIDIOt ya que está escrito en lenguaje C.

El tercer objetivo trataba en aprender el funcionamiento de la Proxmark3, el cual ha sido sencillo debido a que es muy intuitivo y posee documentación sobre su funcionamiento. Este dispositivo posee la capacidad de leer, escribir, emular y atacar la seguridad de tarjetas RFID por lo que su aprendizaje ha supuesto un paso muy importante para comprender completamente la funcionalidad que debe poseer la aplicación desarrollada.

El cuarto objetivo consistía en desarrollar una aplicación compatible con la mayoría de teléfonos con tecnología NFC existentes. Este objetivo no ha sido posible cumplirlo debido a que las tarjetas RFID de tipo Mifare Classic (Mini, 1K o 4K) solo son compatibles si el microchip NFC del teléfono ha sido fabricado por NXP. Para corroborar este punto la aplicación ha sido probada en los teléfonos LG L5 E610, Samsung Galaxy Nexus, Samsung Galaxy S4 y LG Nexus 4, funcionando en los dos primeros pero no en los dos últimos. [55]

El quinto objetivo consistía en leer, escribir, almacenar y emular tarjetas RFID a través del teléfono. Todas estas operaciones han sido desarrolladas a excepción de la emulación debido a que Android restringe el envío libre de comandos NFC del protocolo 14443-3, la autenticación, lectura y escritura ya vienen implementadas a través de unos métodos específicos que deben ser utilizados para interactuar con las tarjetas RFID. Esto también ha influido en el algoritmo Crapto1 ya que la idea inicial era atacar la seguridad de las tarjetas Mifare Classic directamente desde la tecnología NFC del dispositivo móvil. Para solucionar este problema se decidió utilizar la Proxmark3 desde el teléfono conectándola a través del cable USB OTG.

El sexto objetivo hace referencia al desarrollo de una base de datos que gestione toda la información de la aplicación. Ya se poseían conocimientos de SQL, lenguaje parecido al utilizado para la base de datos interna (MySQL). En el backend ha sido utilizado Google App Engine, el cual ofrece almacenar la información en varios lenguajes de programación, que es una gran ventaja para el programador.

Respecto a errores de tipo hardware solamente se produjo uno debido a que para conectar el teléfono Samsung Galaxy Nexus al PC e instalar la aplicación era necesario descargar un driver específico desde la página oficial de Samsung. [19] Esto ocurrió únicamente con ese teléfono.

Finalmente este proyecto ha permitido, desde un punto de vista personal, conocer en profundidad un campo de gran interés, ligado al mundo de la informática y que aún puede expandirse mucho más ya que la tecnología NFC y Android están en pleno auge.

---

## 2. Futuras líneas de trabajo

A continuación se van a explicar una serie de posibles mejoras sobre la aplicación desarrollada:

Crear un servidor centralizado para el almacenamiento de todas las tarjetas RFID, de tal forma que los usuarios las almacenen en dicho servidor y las consulten cuando lo deseen. El teléfono tendría un registro de un número de tarjetas utilizadas frecuentemente que serían almacenadas en el teléfono para su acceso más rápido, mientras que para acceder al resto habría que recogerlas del servidor centralizado. Esto puede prevenir la pérdida de tarjetas almacenadas de manera local en el propio teléfono. Esta mejora también podría aplicarse a las claves y grupos de claves.

Utilizar la aplicación para acceder a servicios de transporte, control de accesos, cerraduras y otros elementos de la vida cotidiana, haciendo que los usuarios no requieran llevar consigo los elementos que actualmente son imprescindibles para estas tareas.

Que la aplicación interactúe con tarjetas a través del protocolo 14443-4, lo que permitiría leer y emular pasaportes electrónicos y tarjetas de crédito. Esta sería una ampliación interesante ya que los pasaportes y tarjetas de crédito son utilizados en el día a día y así serían usados sin necesidad de llevarlos.

Las dos anteriores mejoras requerirían almacenar la información como elemento seguro para que ningún usuario no deseado pudiera acceder a ella y utilizarla de una manera inadecuada.

Hacer la aplicación más accesible para personas con discapacidades, por ejemplo, reconocer los comandos leer y escribir vocalizando las palabras “leer” y “escribir”, respectivamente, pronunciar el nombre con el que se almacenaría la tarjeta, la información a escribir en una tarjeta, etc. De la misma manera la propia aplicación también iría explicando verbalmente la situación en la que se encuentra, cuando termina de realizar una acción, la lista de tarjetas almacenadas, etc.

# REFERENCIAS

---

---

Las referencias consultadas son las siguientes:

- [1] RAE. [www.rae.es](http://www.rae.es)
- [2] Google App Engine. <https://developers.google.com/appengine/>  
<https://appengine.google.com/>
- [3] Google Cloud Platform: <https://cloud.google.com/>
- [4] Google Wallet. <http://googleblog.blogspot.com/2011/09/launching-google-wallet-on-sprint-and.html>
- [5] Wikipedia. <http://es.wikipedia.org>
- [6] Java. <http://www.java.com>
- [7] C++. <http://www.cplusplus.com>
- [8] Oracle Corporation. <http://www.oracle.com>
- [9] Wordreference. <http://www.wordreference.com>
- [10] Microsoft Office 2010. <http://office.microsoft.com/es-es/>
- [11] Visual paradigm. <http://www.visual-paradigm.com/>
- [12] Eclipse. <http://www.eclipse.org>
- [13] Ubuntu. <http://www.ubuntu.com>
- [14] Windows 7. <http://windows.microsoft.com/es-ES/windows7/products/home>
- [15] Asus. <http://www.asus.com>
- [16] Android. <https://www.android.com>
- [17] Open Handset Alliance. <http://www.openhandsetalliance.com>
- [18] Android Developers. <http://developer.android.com>
- [19] Samsung. <http://www.samsung.com>
- [20] Proxmark3. <http://proxmark.org>, [www.proxmark3.com](http://www.proxmark3.com)
- [21] Proxmark3 Manual de Referencia.  
<https://code.google.com/p/proxmark3/wiki/HomePage>

- 
- [22] USB Host Controller.  
<https://play.google.com/store/apps/details?id=hu.sztupy.android.usbhostcontroller&hl=en>
- [23] Complete Linux Installer.  
[https://play.google.com/store/apps/details?id=com.zpwebsites.linuxonandroid&feature=search\\_result#?t=W251bGwsMSwxLDEsImNvbS56cHdlYnNpdGVzLmtpbnV4b25hbmRyb2lklo](https://play.google.com/store/apps/details?id=com.zpwebsites.linuxonandroid&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS56cHdlYnNpdGVzLmtpbnV4b25hbmRyb2lklo).
- [24] Android Terminal Emulator.  
<https://play.google.com/store/apps/details?id=jackpal.androidterm>
- [25] Root Explorer.  
<https://play.google.com/store/apps/details?id=com.speedsoftware.rootexplorer>
- [26] LibNFC. <http://nfc-tools.org/index.php?title=Libnfc>  
<http://code.google.com/p/libnfc/>
- [27] RFIDIOT. <http://rfidiot.org/>
- [28] Android CyanogenMod. <http://www.cyanogenmod.org>
- [29] VMWare Player. <https://www.vmware.com/es/products/player>
- [30] Crapto1. <http://code.google.com/p/crapto1/>
- [31] Mfoc. <https://code.google.com/p/mfoc/>
- [32] Mfoc GUI. <https://github.com/Huuf/OV-mfoc-GUI/tree/master/mfocGUI>
- [33] Camtasia Studio. <http://www.techsmith.com/camtasia.html>
- [34] Andy Rubin. Where's my Gphone?.  
<http://googleblog.blogspot.com.es/2007/11/wheres-my-gphone.html>
- [35] NFC fórum. [http://www.nfc-forum.org/aboutnfc/nfc\\_and\\_contactless](http://www.nfc-forum.org/aboutnfc/nfc_and_contactless)
- [36] Cyclopaedia. <http://www.cyclopaedia.es/>
- [37] Seas. <http://www.seas.es/blog/>
- [38] Stackoverflow. <http://stackoverflow.com/>

- 
- [39] Bueno Delgado, M<sup>a</sup> Victoria. Pavón Mariño, Pablo. De Gea García, Alfonso. La tecnología NFC y sus aplicaciones en un entorno universitario, Universidad Politécnica de Cartagena, 2011
- [40] Ceballos Villach, Jordi. NFC Fundamentos y Aplicaciones, Universidad Oberta de Cataluña, 2013
- [41] Antipolis, Sophia. NFCIP-1 Security Standard Protects Near Field Communication, 4<sup>th</sup> ETSI Security Workshop, 2009
- [42] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling MIFARE Classic, Instituto de Informática y Ciencias de la Información - Universidad de Radboud Nijmegen, 2008.
- [43] Flavio D. Garcia, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card, Universidad de Radboud Nijmegen, 2009.
- [44] Pedro Peris-López, Agustín Orfila, Julio C. Hernández-Castro and Jan C. A. van der Lubbe. Flaws on RFID grouping-proofs. Guidelines for future sound protocols, Journal Network and Computer Applications, 2009.
- [45] Karsten Nohl, David Evans, Starbug Starbug, Henryk Plötz. Reverse-Engineering a Cryptographic RFID Tag, Departamento de Ciencias de la Computación – Universidad de Virginia y Chaos Computer Club, 2008
- [46] Karsten Nohl. Cryptanalysis of Crypto1, Universidad de Virginia
- [47] NXP. MIFARE Classic EV1 1K – Main stream contactless smart card IC for fast and easy solution development, Rev. 3.0, 2014
- [48] NXP. MIFARE Ultralight contactless single-ticket IC, Rev. 3.9, 2014
- [49] Gerhard de Koning Gans, Jaap-Henk Hoepman, Flavio D. Garcia. A Practical Attack on the Mifare Classic, Instituto de Informática y Ciencias de la Información – Universidad de Radboud Nijmegen, 2008
- [50] Wee Hon Tan. Practical Attacks on the MIFARE Classic, Departamento de Informática – Escuela Imperial de Londres, 2009
- [51] Mifare.net. <http://www.mifare.net>

- 
- [52] NXP. PN532 User Manual Rev. 02
  - [53] NXP. PN533 User Manual Rev. 03
  - [54] NXP. <http://www.nxp.com>
  - [55] Compatibility Issues with Mifare Classic 1K NFC Tags. <http://www.rfid-blog.com/?p=2247>
  - [56] Online Hex Editor. <http://www.onlinehexeditor.com/>



# ANEXOS

---

# ANEXO I:

## Acrónimos y Definiciones

---

En el presente apartado se van a mostrar los acrónimos y definiciones que se van a usar a lo largo de toda la memoria.

## 1. Acrónimos

Acrónimo	Significado
AC	Anticollision Command
ACID	Atomic, Consistent, Isolated, and Durable
ADT	Android Developer Tools
AES	Advanced Encryption Standard
API	Application Programming Interface
APK	Android Package
ATQA	Answer To reQuest Type A
AVD	Android Virtual Device
BSD	Berkeley Software Distribution
CU	Caso de Uso
DES	Data Encryption Standard
DEX	Dalvik Executables
EAL	Evaluation Assurance Level
ECJ	Eclipse Compile for Java
GAE	Google App Engine
GPS	Global Positioning System
GUI	Graphic User Interface
HCE	Host Card Emulation
HF	High Frequency
IDE	Integrated Development Environment
JDT	Java Development Toolkit
JVM	Java Virtual Machine
LFSR	Linear Feedback Shift Register
MFOC	MiFare classic Offline Cracker
MVC	Modelo Vista Controlador
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP	NFC Interface and Protocol
PC	Personal Computer
PCD	Proximity Coupling Devices
POR	Power On Reset
REQA	REQuest command Type A
RF	Requisito Funcional
RFID	Radio Frequency Identificator
RNF	Requisito No Funcional
RNG	Random Number Generation
RTD	Record Type Definition
RUC	Requisito de Usuario de Capacidad

<b>RUR</b>	Requisito de Usuario de Restricción
<b>SDK</b>	Software Development Kit
<b>SGL</b>	Scalable Graphics Library
<b>SSL</b>	Secure Sockets Layer
<b>TISC</b>	Tarjetas inteligentes sin contacto
<b>UID</b>	Identificador único
<b>UML</b>	Unified Modeling Language
<b>URI</b>	Uniform Resource Identifier
<b>USB</b>	Universal Serial Bus
<b>USB OTG</b>	USB On-The-Go
<b>VCD</b>	Vicinity Coupling Devices
<b>WUPA</b>	Wake UP command Type A

Tabla 243: Acrónimos

## 2. Definiciones

- **AES:** algoritmo para cifrar información que utiliza el cifrado por bloques.
- **Android:** sistema operativo basado en Linux para dispositivos móviles, tales como teléfonos inteligentes o tablets. Fue desarrollado inicialmente por Android Inc., una firma comprada por Google en 2005. Es el principal producto de la Open Handset Alliance.
- **API:** consiste en un conjunto de llamadas que ofrecen acceso a funciones y procedimientos representando una capa de abstracción para el desarrollador.
- **App:** Abreviatura de aplicación, muy utilizada cuando se refiere a aplicaciones en terminales móviles.
- **Bytecode:** es un código intermedio más abstracto que el código máquina.
- **Crypto1:** implementaciones abiertas de ataques contra el sistema de cifrado Crypto1.
- **Crypto1:** algoritmo utilizado por las tarjetas RFID de tipo Mifare Classic para encriptar su información.
- **Dalvik:** es la máquina virtual que utiliza la plataforma para dispositivos móviles Android. Dalvik ha sido diseñada por Dan Bornstein con contribuciones de otros ingenieros de Google. Dalvik está optimizada para requerir poca memoria y está diseñada para permitir ejecutar varias instancias de una máquina virtual simultáneamente, delegando en el sistema operativo subyacente el soporte de aislamiento de procesos, gestión de memoria e hilos.
- **DES:** algoritmo para cifrar información.

- **Framework:** término con el que se define un amplio conjunto de elementos que permite el desarrollo y organización de software utilizando un determinado lenguaje o tecnología.
- **Google App Engine:** servicio de alojamiento web que presta Google de forma gratuita hasta determinadas cuotas.
- **GPS:** es un sistema de navegación que mediante satélites permite ubicar un elemento en una latitud y longitud con un pequeño error de precisión.
- **GUI:** se denomina así a la parte del software que mediante el uso de elementos gráficos ofrece al usuario la posibilidad de interactuar con el sistema.
- **HCE:** herramienta de Android que permite emular la norma ISO/IEC 7816 basado en tarjetas inteligentes que utilizan el protocolo ISO/IEC 14443-4.
- **Java:** es un lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems a principios de los años 90. El lenguaje en sí mismo toma mucha de su sintaxis de C y C++, pero tiene un modelo de objetos más simple y elimina herramientas de bajo nivel, que suelen inducir a muchos errores, como la manipulación directa de punteros o memoria.
- **JVM:** es una máquina virtual de proceso nativo, es decir, ejecutable en una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en un código binario especial (el Java bytecode), el cual es generado por el compilador del lenguaje Java.
- **Kernel:** núcleo de un sistema operativo y por lo tanto, pieza clave para el funcionamiento del mismo. Responsable de dar acceso al hardware, gestionar recursos y hacer llamadas al sistema.
- **Lector RFID:** dispositivo con tecnología RFID que permite leer tarjetas con su misma tecnología.
- **LFSR:** registro de desplazamiento en el cual la entrada es un bit proveniente de aplicar una función de transformación lineal a un estado anterior.
- **Man-In-The-Middle:** tipo de ataque informático en el que el atacante se posiciona entre el emisor y el receptor de la información y puede escuchar e incluso modificar la información que intercambian.
- **Máquina Virtual:** en informática una máquina virtual es un software que emula a una computadora y puede ejecutar programas como si fuese una computadora real. Este software en un principio fue definido como “un duplicado eficiente y aislado de una máquina física”.

- **Microsoft Excel:** es una aplicación distribuida por Microsoft Office para hojas de cálculo. Este programa es desarrollado y distribuido por Microsoft, y es utilizado normalmente en tareas financieras y contables.
- **Microsoft Office:** es una suite de oficina que abarca e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos Microsoft Windows y Mac OS X.
- **Mifare:** es la tecnología de tarjetas inteligentes sin contacto (TISC) más ampliamente instalada en el mundo con aproximadamente 250 millones de TISC y 1.5 millones de módulos lectores vendidos. Es equivalente a las 3 primeras partes de la norma ISO 14443 Tipo A de 13,56 MHz con protocolo de alto nivel. La distancia típica de lectura es de 10 cm (unas 4 pulgadas). La distancia de lectura depende de la potencia del módulo lector, existiendo lectores de mayor y menor alcance.
- **Modelo Vista Controlador:** es un patrón o modelo de abstracción de desarrollo de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de negocio en tres componentes distintos.
- **NFC:** tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos a menos de 10cm. Es una simple extensión del estándar ISO 14443 (RFID).
- **NFC Forum:** se creó en 2004 por las tres compañías pioneras de la tecnología NFC: Philips, Sony y Nokia, para avanzar en las especificaciones de esta tecnología. Actualmente, cuenta con más de 160 miembros que representan a fabricantes, desarrolladores de aplicaciones software, vendedores, instituciones financieras, agencias gubernamentales, consorcios de transporte y organizaciones sin ánimo de lucro.
- **Open Headset Alliance:** es una alianza comercial de 78 compañías para desarrollar estándares abiertos para dispositivos móviles.
- **Plugin:** pieza de software que se relaciona y ejecuta con otro para aportarle una función nueva y específica.
- **Proceso:** un proceso es un programa en ejecución, y representa la unidad de procesamiento básica gestionada por el sistema operativo.
- **Proxmark3:** herramienta de tecnología RFID diseñada para espiar, escuchar y emular tarjetas RFID.
- **RFID:** es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

- 
- **SDK:** es un conjunto de elementos para el desarrollo de aplicaciones de software.
  - **Sistema Operativo:** Software cuya finalidad principal es simplificar el manejo de un elemento con capacidad computacional, gestionando sus recursos, ofreciendo servicios y ejecutando mandatos del usuario.
  - **Smartphone:** es un término comercial para denominar a un teléfono móvil que ofrece más funciones que un teléfono celular común.
  - **Tarjeta RFID:** dispositivos que contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un lector RFID.

# ANEXO II:

## Gestión del Proyecto

---



## 1. Planificación del Proyecto

El proyecto se comenzó el día 27 de Junio del 2014 y ha finalizado el día 4 de Enero del 2015, una duración de 137 días sin tener en cuenta los fines de semana pero sí los días festivos entre semana.

Se debe señalar que durante este periodo no se ha mantenido una jornada de trabajo estable ya que por motivos laborales el tiempo de trabajo ha ido variando según la disponibilidad que se ha tenido, la mayoría de las semanas se empleaba una jornada de dos horas diarias, algunas de 4 ó 1 hora y en ocasiones era imposible realizar tarea alguna.

A continuación se muestra el diagrama de Gantt del proyecto, incluyendo las subtarefas de cada fase con sus respectivas duraciones y periodos de tiempo:

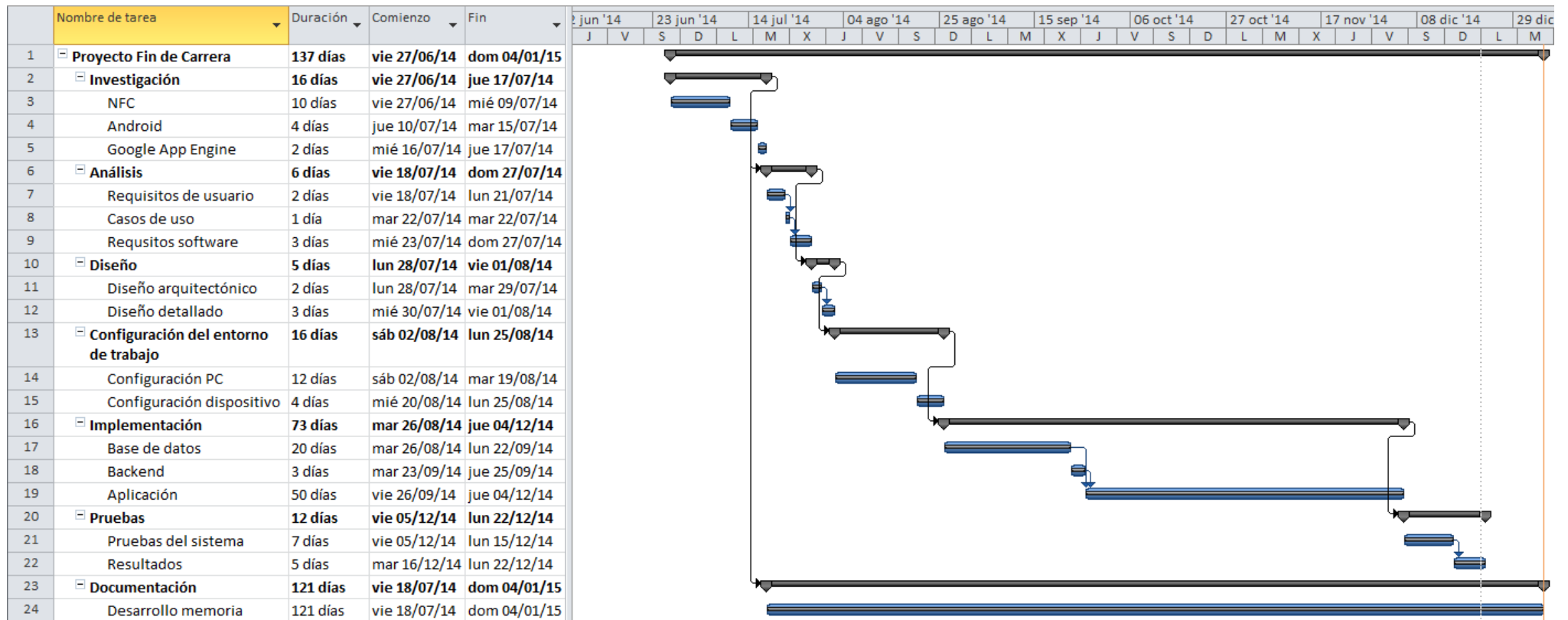


Ilustración 32: Diagrama de Gantt

## 2. Presupuesto del Proyecto

En este apartado se detalla el presupuesto que cubre todos los costes y las necesidades que se plantean a lo largo de la evolución del proyecto.

### 2.1. Coste del personal

A continuación se calculará el coste del personal con una dedicación de un solo hombre al mes.

Fase	Rol	Coste (€/hora)	Horas/día	Días	Coste total (€)
Investigación	Analista	40	2	16	1280
Análisis	Analista	40	2	6	480
Diseño	Analista	40	2	5	400
Configuración del entorno de desarrollo	Programador	35	2	16	1120
Implementación	Programador	35	2	73	5110
Pruebas	Programador	35	2	12	840
Documentación	Analista	40	2	121	9680
<b>TOTAL</b>					<b>18910</b>

Tabla 244: Coste del personal

### 2.2. Coste de equipos

A continuación se mostrará una tabla en la que se detallarán los costes de los equipos informáticos empleados para el proyecto así como otros dispositivos electrónicos.

Descripción	Coste (€)/Unidad	Unidades	Coste total (€)	Periodo de amortización (meses)	Duración proyecto (meses)	Coste asociado (€)
Portátil Asus N53S	869,00	1	869,00	24	6	217,25
Touchatag	19,99	1	19,99	24	6	5,00
Proxmark3	183,94	1	183,94	24	6	45,99
Tarjetas RFID	0,52	4	2,08	24	6	0,52
Samsung Galaxy Nexus	300,00	1	300,00	24	6	75,00
USB OTG	1,99	1	1,99	24	6	0,50
Antena HF	47,39	1	47,39	24	6	11,85
<b>TOTAL</b>						<b>356,10</b>

Tabla 245: Coste del equipo

### 2.3. Coste de software

En la tabla siguiente se mostrará en detalle los costes del software adquirido para este proyecto.

Descripción	Coste (€)/ Unidad	Unidades	Coste total (€)	Periodo de amortización (meses)	Duración proyecto (meses)	Coste asociado (€)
Eclipse	0,00	1	0,00	24	6	0,00
Android CyanogenMod	0,00	1	0,00	24	6	0,00
Android SDK	0,00	1	0,00	24	6	0,00
USB Host Controller	0,00	1	0,00	24	6	0,00
Complete Linux Installer	0,00	1	0,00	24	6	0,00
Android Terminal Emulator	0,00	1	0,00	24	6	0,00
Explorer	0,00	1	0,00	24	6	0,00
LibNFC	0,00	1	0,00	24	6	0,00
Licencia de Microsoft Office 2010 Hogar y Estudiantes	119,00	1	119,00	24	6	29,75
Licencia de Microsoft Windows 7 Home Premium	349,00	1	349,00	24	6	87,25
Visual paradigm Community Edition	0,00	1	0,00	24	6	0,00
VMware Player	0,00	1	0,00	24	6	0,00
MiFare classic Offline Cracker	0,00	1	0,00	24	6	0,00
Camtasia Studio 8	0,00	1	0,00	24	6	0,00
Mifare Classic Offline Cracker GUI	0,00	1	0,00	24	6	0,00
<b>TOTAL</b>						<b>117,00</b>

Tabla 246: Coste del software

### 2.4. Material fungible

A continuación se muestra el presupuesto dedicado al material de oficina de este proyecto.

Descripción	Coste total (€)
Material de papelería	40,00
<b>TOTAL</b>	<b>40,00</b>

Tabla 247: Coste del material fungible

### 2.5. Costes directos totales

A continuación se detallan los costes totales del proyecto.

Descripción	Coste total (€)
Personal	18910,00
Equipo	356,10
Software	117,00
Material fungible	40,00
<b>TOTAL</b>	<b>19423,10</b>

Tabla 248: Costes totales

## 2.6. Costes indirectos

A continuación aparece reflejado los costes indirectos con un margen del 2%.

Gastos totales (€)	Margen de costes indirectos	Total de riesgos (€)
19423,10	2%	388,46

Tabla 249: Coste indirectos

## 2.7. Beneficio

Al ser un proyecto académico no se realiza con ánimo de lucro, por lo que el beneficio será de 0€.

## 2.8. Margen de riesgo

A continuación aparece reflejado los costes del margen de riesgo de un 15%.

Gastos totales (€)	Coste de margen de riesgo	Total de riesgos (€)
19423,10	15%	2913,46

Tabla 250: Coste del margen de riesgo

## 2.9. Presupuesto total

Por último, se va a mostrar un resumen del presupuesto con la suma de todos los costes asociados al proyecto. Destacar que el IVA aplicado al presupuesto del proyecto es del 21%.

Descripción	Coste sin IVA (€)	IVA (€)	Coste con IVA (€)
Costes totales	19423,10	4078,85	23501,95
Costes indirectos	388,46	81,58	470,04
Beneficio	0	0,00	0,00
Riesgos	2913,46	611,83	3525,29
<b>TOTAL</b>	<b>22725,02</b>	<b>4772,26</b>	<b>27497,28</b>

Tabla 251: Resumen del presupuesto del proyecto

El coste total del proyecto es de 27.497,28 € (VEINTISIETE MIL CUATROCIENTOS NOVENTA Y SIETE CON VEINTIOCHO EUROS).

# ANEXO III:

## Manual de Usuario

---

Este manual de usuario es una guía para utilizar la aplicación NFC en cualquier dispositivo móvil que contenga la tecnología NFC.

**Nota1:** es recomendable la lectura íntegra del manual para comprender mejor el sistema.

**Nota2:** es recomendable no remover la tarjeta RFID una vez que la operaciones de lectura y escritura han sido iniciadas para evitar daños en la propia tarjeta.

## 1. Acceso Inicial

Se debe acceder al menú de aplicaciones del dispositivo móvil y localizar el icono de la aplicación llamado NFC como se muestra en la siguiente imagen.

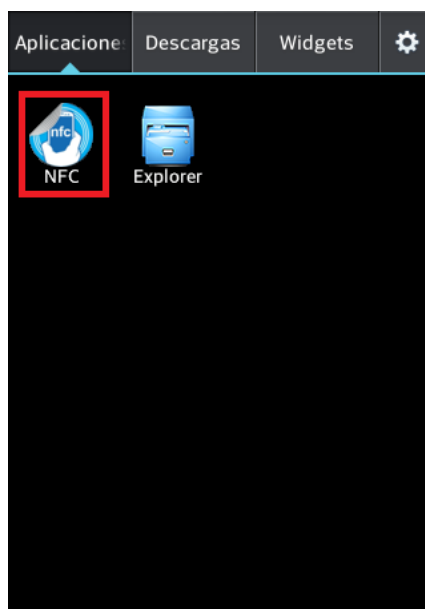


Ilustración 33: Manual de usuario – Acceso inicial

Al pinchar sobre el icono se abrirá la pantalla inicial de la aplicación.

## 2. Pantalla Principal

En la pantalla inicial se pueden seleccionar cinco opciones: Leer, Escribir, Ver tarjetas escaneadas, Claves y Estadísticas, las cuales están explicadas en los apartados 3, 4, 5, 6 y 7, respectivamente, de este manual.



Ilustración 34: Manual de usuario – Pantalla inicial

**Nota:** sólo se podrá leer o escribir una tarjeta RFID si la tecnología NFC del dispositivo está activada.

### 3. Leer

Esta funcionalidad consiste en leer el contenido de una tarjeta RFID, y si se desea, guardar su contenido en el dispositivo móvil.

Para leer una tarjeta hay que pinchar sobre el icono de la operación leer.

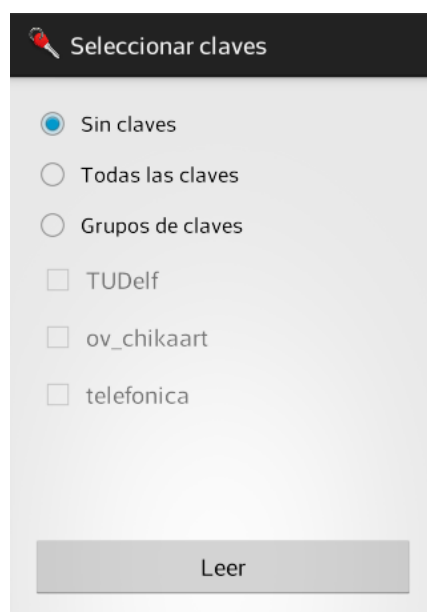


Ilustración 35: Manual de usuario – Acceder a leer



Posteriormente es necesario seleccionar las claves con las que la tarjeta será autenticada y hacer click sobre el botón Leer. Existen tres opciones en la selección de claves:

- **Sin claves:** no se utilizará ninguna clave.
- **Todas las claves:** se utilizarán todas las claves almacenadas en el dispositivo móvil.
- **Grupos de claves:** únicamente se utilizaran las claves pertenecientes a los grupos de claves seleccionados.



**Ilustración 36:** Manual de usuario – Selección de claves en lectura

Por último hay que acercar la tarjeta RFID a leer a la parte posterior del dispositivo móvil, aparecerá el mensaje “Leyendo tag. Por favor espere...” mientras la lectura continúe. Cuando termine aparecerá la información leída en formato hexadecimal.

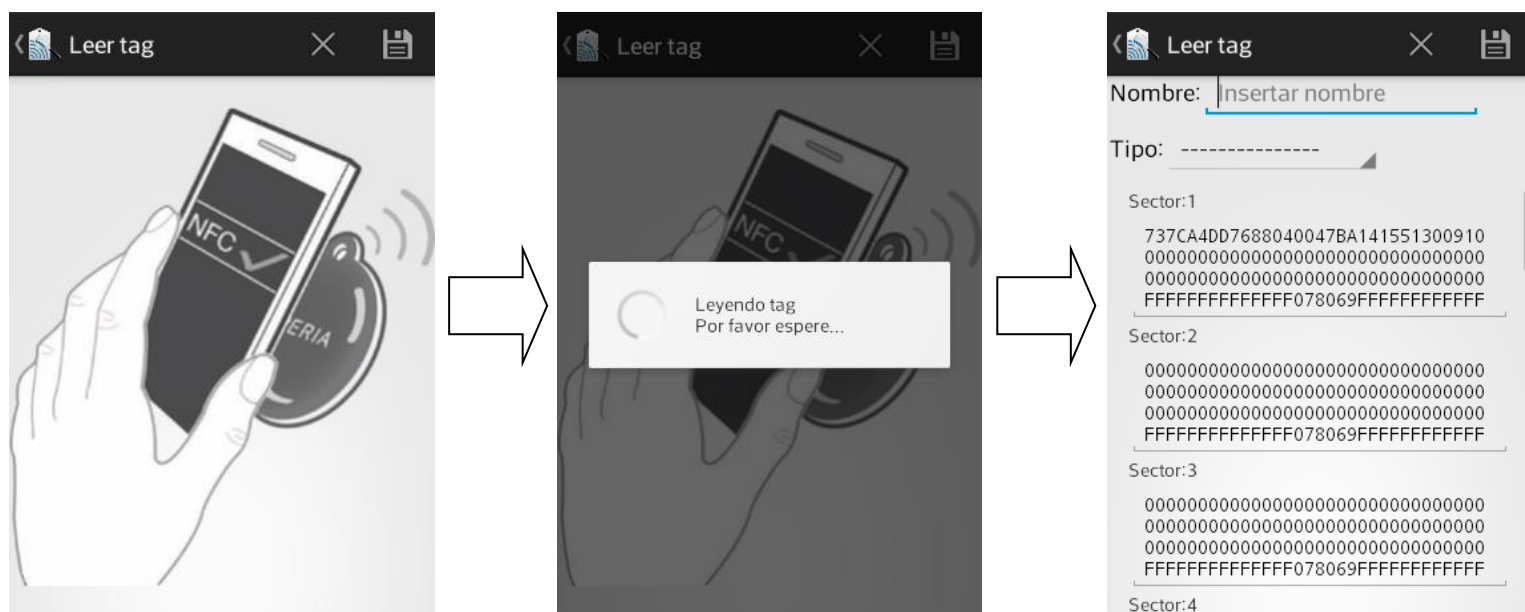


Ilustración 37: Manual de usuario – Leer tarjeta

Si el contenido de un bloque puede ser autenticado pero no leído se mostrará con 32 guiones (-----).

Una vez que la tarjeta ha sido leída existe la posibilidad de borrar el contenido leído o almacenarla en el dispositivo móvil.

Para borrar el contenido hay que hacer click sobre la opción Limpiar en el menú de opciones y la pantalla volverá a encontrarse en la situación anterior de acercar la tarjeta RFID al dispositivo móvil.

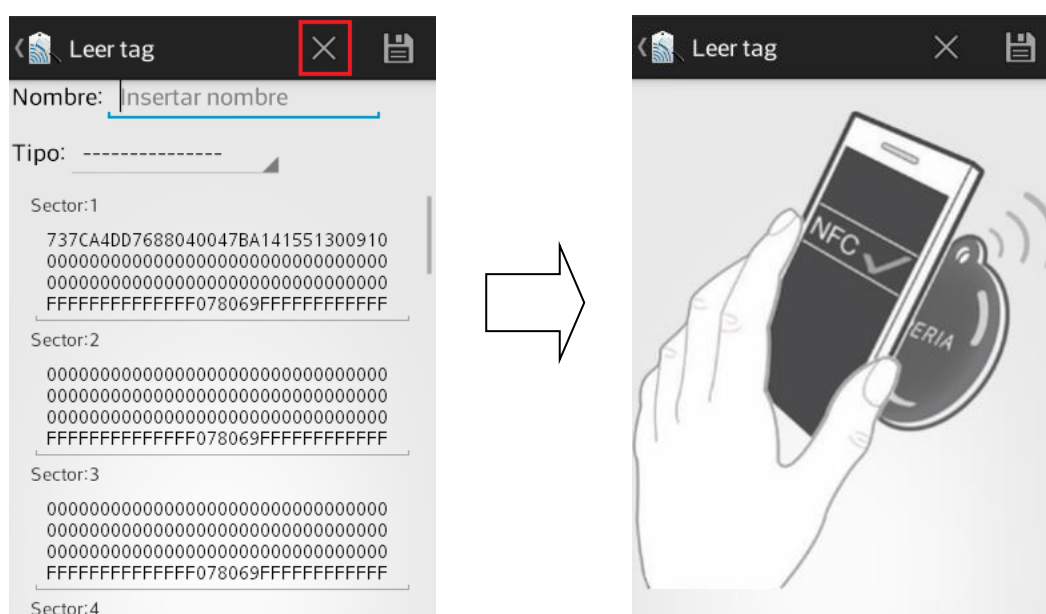


Ilustración 38: Manual de usuario – Limpiar lectura

Para ello se debe rellenar la siguiente información:

- **Nombre:** contendrá el nombre de la tarjeta. Este campo será único e irrepetible de entre todas las tarjetas almacenadas en el dispositivo.
- **Tipo:** valor de clasificación de la tarjeta dentro del dispositivo móvil. Por defecto la aplicación solo tiene “Control de acceso”, “Pasaporte” y “Transporte”.
- **Contenido de la tarjeta:** corresponde con el contenido de la tarjeta RFID. Por defecto es el resultado de la lectura de la tarjeta. Cada bloque debe contener 32 caracteres hexadecimales (del 0 al 9 y ABCDEF).



Ilustración 39: Manual de usuario – Contenido tarjeta a guardar

Si se quiere seleccionar un tipo de tarjeta diferente existe la opción “--Nuevo tipo--” entre las opciones por defecto. Al seleccionar esta opción aparecerá un diálogo donde escribir el nombre del nuevo tipo y posteriormente aceptar la operación.

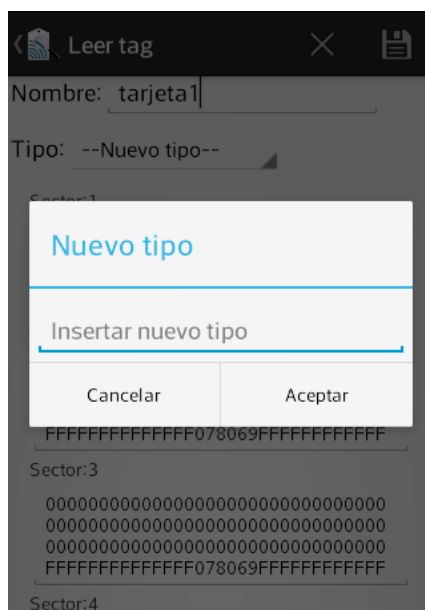


Ilustración 40: Manual de usuario – Nuevo tipo de tarjeta

Una vez que el nombre, tipo y contenido de la tarjeta han sido rellenados se hace click en la opción Guardar del menú de opciones.

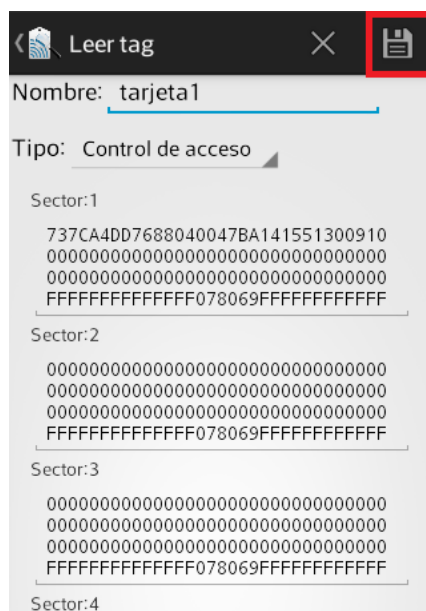


Ilustración 41: Manual de usuario – Guardar tarjeta

Si la tarjeta ha sido almacenada correctamente aparecerá el mensaje “Tag almacenado”, sino un mensaje con el error producido.

Cuando se intenta almacenar una tarjeta puede ocurrir que ya exista una guardada con ese mismo nombre. En este caso aparecerá un diálogo ofreciendo dos opciones:

- **Renombrar tarjeta:** se renombrará la tarjeta que se desea guardar.

- **Reemplazar tarjeta:** la tarjeta antigua será sustituida por la nueva.



**Ilustración 42: Manual de usuario – Tarjeta repetida**

Si se escoge la opción Renombrar aparecerá otro diálogo solicitando el nuevo nombre de la tarjeta y una vez introducida se almacenará la tarjeta. Si se escoge Reemplazar la tarjeta será almacenada sustituyendo a la anterior.

### 3.1. Ver como transporte

Una vez que la tarjeta ha sido leída (ver apartado 3 Leer) o abierta para edición (ver apartado 5.2 Editar tarjeta) se puede ver su contenido de transporte si la tarjeta lo posee.

Para ello hay que hacer click sobre la opción “Ver como tarjeta de transporte”.

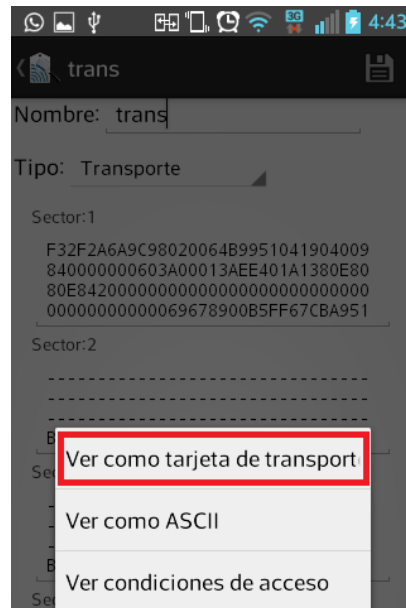


Ilustración 43: Manual de usuario – Ver como transporte – Opción menú

Si la tarjeta no fuera de transporte aparecería el mensaje “Este tag no es de transporte”.


La vista de transporte posee tres secciones:

- **General:** contiene información de tipo genérico: identificador interno, tipo, producto al que pertenece y el importe disponible en la tarjeta.



Ilustración 44: Manual de usuario – Ver como transporte - General

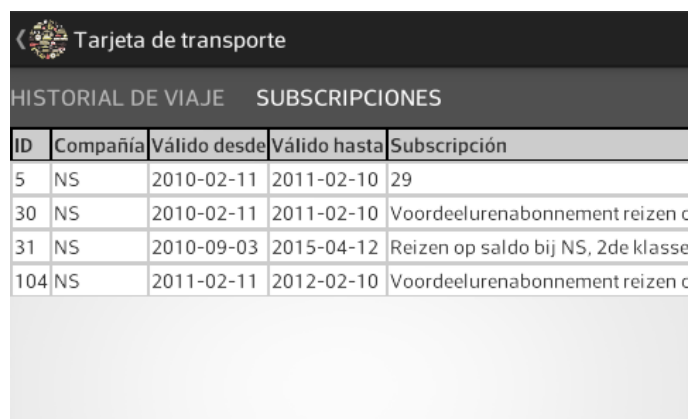
- **Historial:** muestra la información de los viajes que el usuario ha hecho con esta tarjeta de transporte. Contiene el identificador, fecha y hora, compañía, vehículo, máquina, importe y la estación del viaje.



Tarjeta de transporte							
GENERAL		HISTORIAL DE VIAJE			SUBSCRIPCIONES		
ID	Fecha	Hora	Compañía	Transferencia	Vehículo	Máquina	Imp
131	2011-03-20	15:58	NS	check-out	ID: 0	ID: 1258225	1.3
133	2011-03-20	18:03	HTM	check-out	ID: 3101	ID: 1312995	1.8
135	2011-03-21	16:18	RET	check-out	ID: 305	ID: 1319592	1.0
137	2011-04-03	15:39	Connexion	check-out	ID: 1204	ID: 1314243	1.7
139	2011-04-05	18:03	NS	check-out	ID: 0	ID: 1249032	1.3
181	2011-11-27	17:44	Connexion	check-out	ID: 4636	ID: 1313963	1.4
183	2011-12-09	19:56	HTM	check-out	ID: 3006	ID: 1312900	1.8
176	2011-12-11	9:38	NS	no-data	ID: 0	ID: 460833	5.0

Ilustración 45: Manual de usuario – Ver como transporte - Historial

- **Subscripciones:** enseña las subscripciones a las que el usuario se ha registrado con esta tarjeta. Contiene el identificador, compañía, fecha inicio, fecha fin y la descripción de la subscripción.

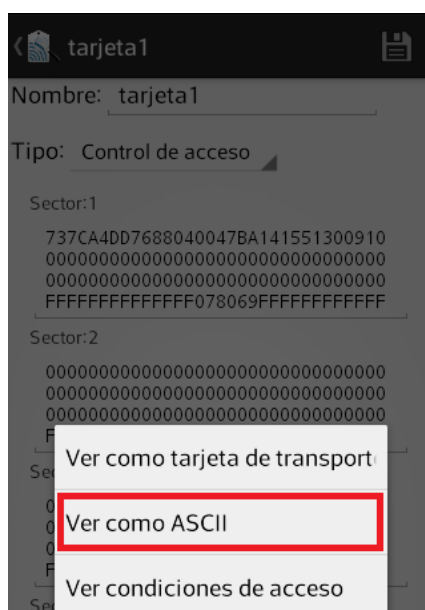


Tarjeta de transporte				
HISTORIAL DE VIAJE		SUBSCRIPCIONES		
ID	Compañía	Válido desde	Válido hasta	Subscripción
5	NS	2010-02-11	2011-02-10	29
30	NS	2010-02-11	2011-02-10	Voordeelurenabonnement reizen c
31	NS	2010-09-03	2015-04-12	Reizen op saldo bij NS, 2de klasse
104	NS	2011-02-11	2012-02-10	Voordeelurenabonnement reizen c

Ilustración 46: Manual de usuario – Ver como transporte - Subscripciones

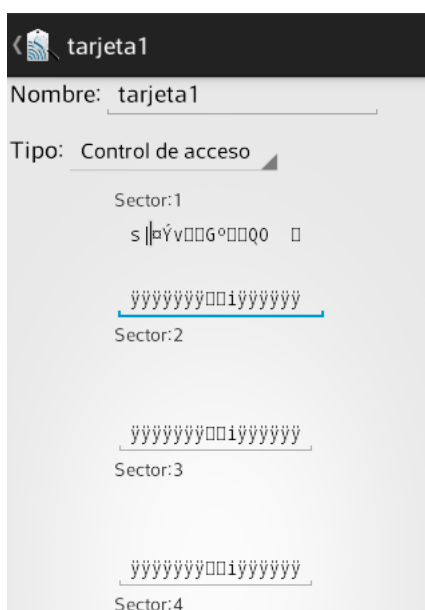
### 3.2. Ver como ASCII

Una vez que la tarjeta ha sido leída (ver apartado 3 Leer) o abierta para edición (ver apartado 5.2 Editar tarjeta) su contenido puede ser visto con formato legible haciendo click sobre la opción “Ver como ASCII”.



**Ilustración 47: Manual de usuario – Ver como ASCII – Opción menú**

Con esta opción la pantalla sigue teniendo la misma estructura pero el contenido de la tarjeta es legible.



**Ilustración 48: Manual de usuario – Ver como ASCII – Contenido en ASCII**

Para volver a ver el contenido en hexadecimal hay que seleccionar la opción “Ver como HEX” en el menú de opciones.



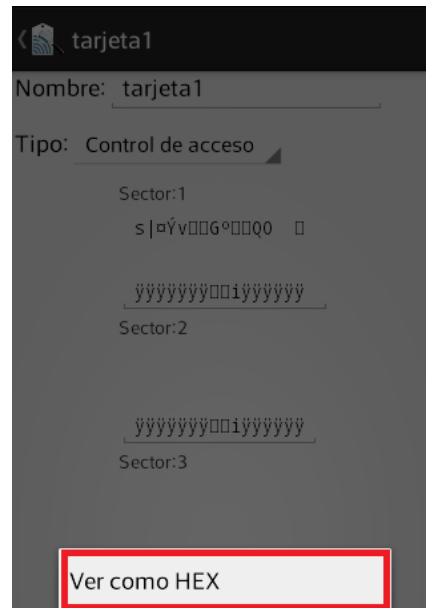


Ilustración 49: Manual de usuario – Ver como ASCII – Contenido en ASCII

### 3.3. Ver condiciones de acceso

Una vez que la tarjeta ha sido leída (ver apartado 3 Leer) o abierta para edición (ver apartado 5.2 Editar tarjeta) se pueden ver sus condiciones de acceso haciendo click sobre la opción “Ver condiciones de acceso”.

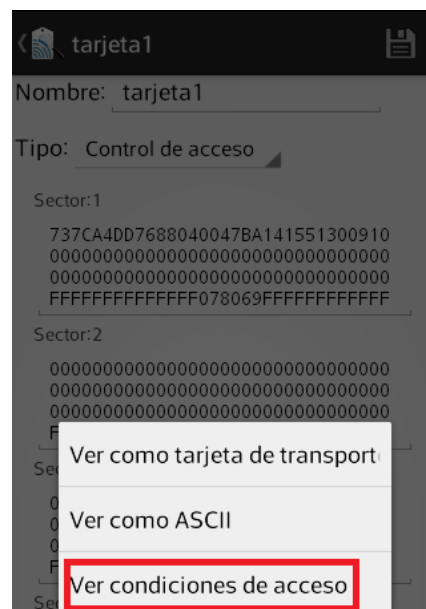
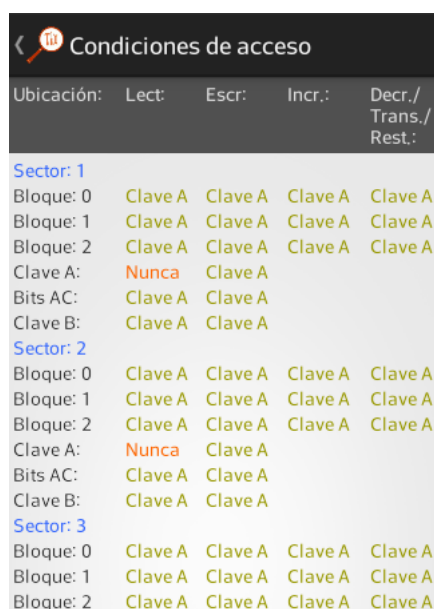


Ilustración 50: Manual de usuario – Ver condiciones de acceso – Opción menú

Esta pantalla muestra el tipo de clave (A, B, ambas o ninguna) que se necesita para realizar una operación sobre cada bloque de la tarjeta.



Ubicación:	Lect:	Escr:	Incr.:	Decr./ Trans./ Rest.:
<b>Sector: 1</b>				
Bloque: 0	Clave A	Clave A	Clave A	Clave A
Bloque: 1	Clave A	Clave A	Clave A	Clave A
Bloque: 2	Clave A	Clave A	Clave A	Clave A
Clave A:	Nunca	Clave A		
Bits AC:	Clave A	Clave A		
Clave B:	Clave A	Clave A		
<b>Sector: 2</b>				
Bloque: 0	Clave A	Clave A	Clave A	Clave A
Bloque: 1	Clave A	Clave A	Clave A	Clave A
Bloque: 2	Clave A	Clave A	Clave A	Clave A
Clave A:	Nunca	Clave A		
Bits AC:	Clave A	Clave A		
Clave B:	Clave A	Clave A		
<b>Sector: 3</b>				
Bloque: 0	Clave A	Clave A	Clave A	Clave A
Bloque: 1	Clave A	Clave A	Clave A	Clave A
Bloque: 2	Clave A	Clave A	Clave A	Clave A

Ilustración 51: Manual de usuario – Ver condiciones de acceso

## 4. Escribir

Esta funcionalidad consiste en escribir el contenido de una tarjeta RFID almacenada en el dispositivo móvil en una tarjeta RFID real.

Para escribir una tarjeta hay que pinchar sobre el icono de la operación escribir.



Ilustración 52: Manual de usuario – Acceder a escribir

Aparecerá un listado con todas las tarjetas almacenadas en el teléfono ordenadas en orden alfabético y clasificadas según el tipo de tarjeta. Hay que seleccionar la que se desea escribir.

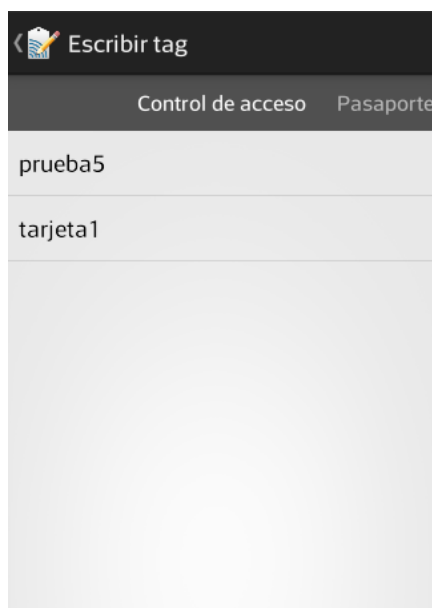


Ilustración 53: Manual de usuario – Seleccionar tarjeta a escribir

Posteriormente es necesario seleccionar las claves con las que la tarjeta será autenticada y hacer click sobre el botón Escribir. Existen tres opciones en la selección de claves:

- **Sin claves:** no se utilizará ninguna clave.
- **Todas las claves:** se utilizarán todas las claves almacenadas en el dispositivo móvil.
- **Grupos de claves:** únicamente se utilizaran las claves pertenecientes a los grupos de claves seleccionados.

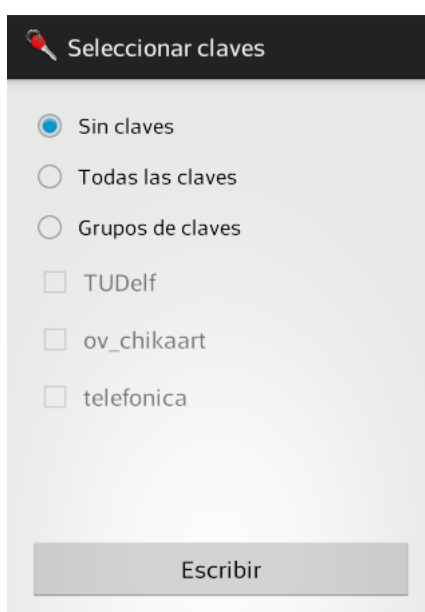
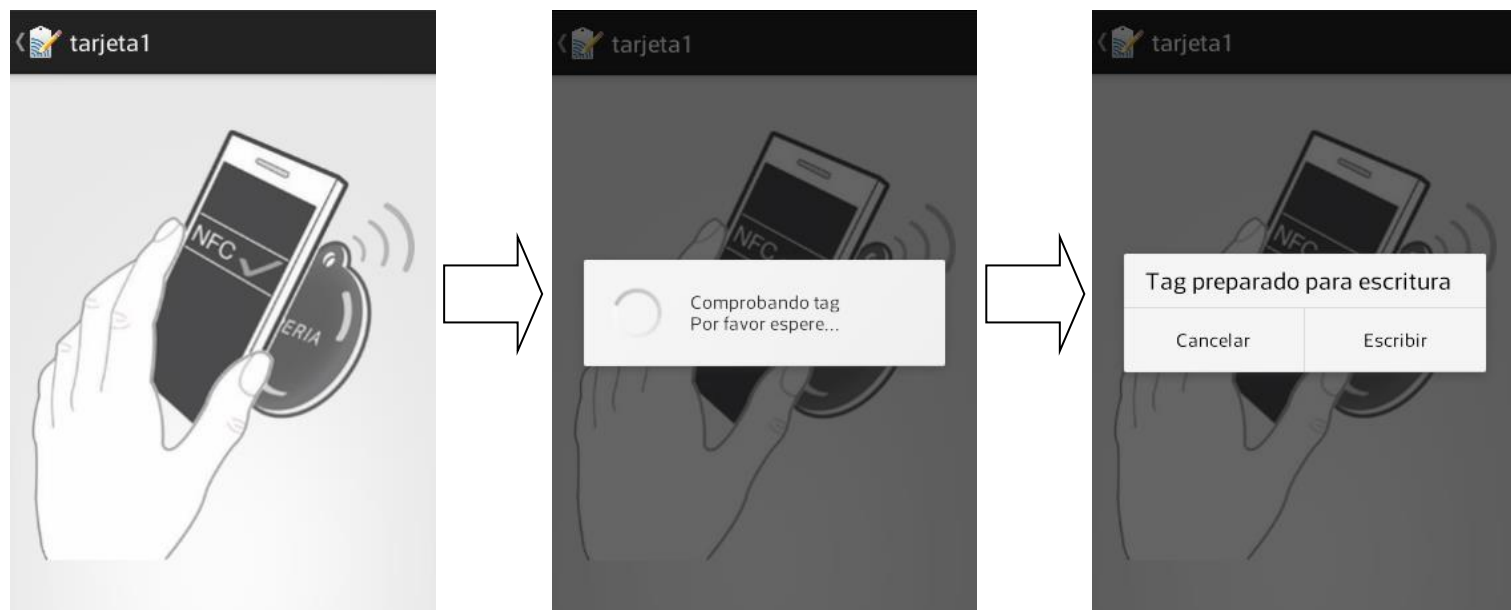


Ilustración 54: Manual de usuario – Selección de claves en escritura

A continuación hay que acercar la tarjeta RFID donde se va a escribir.

El dispositivo comprueba si todos los bloques pueden ser autenticados y escritos, y si la tarjeta posee suficiente tamaño y la información a escribir es compatible mientras aparece el mensaje “Comprobando tag. Por favor espere...”. Si es así aparecerá un diálogo indicando que la escritura está preparada para realizarse y hacer click sobre el botón Escribir para finalizar la operación.



**Ilustración 55: Manual de usuario – Confirmación escritura**

Si algún bloque no puede ser escrito aparecerá un diálogo indicándolo junto con su motivo y dando la opción de cancelar la operación o de escribir todos los bloques que sean posibles.

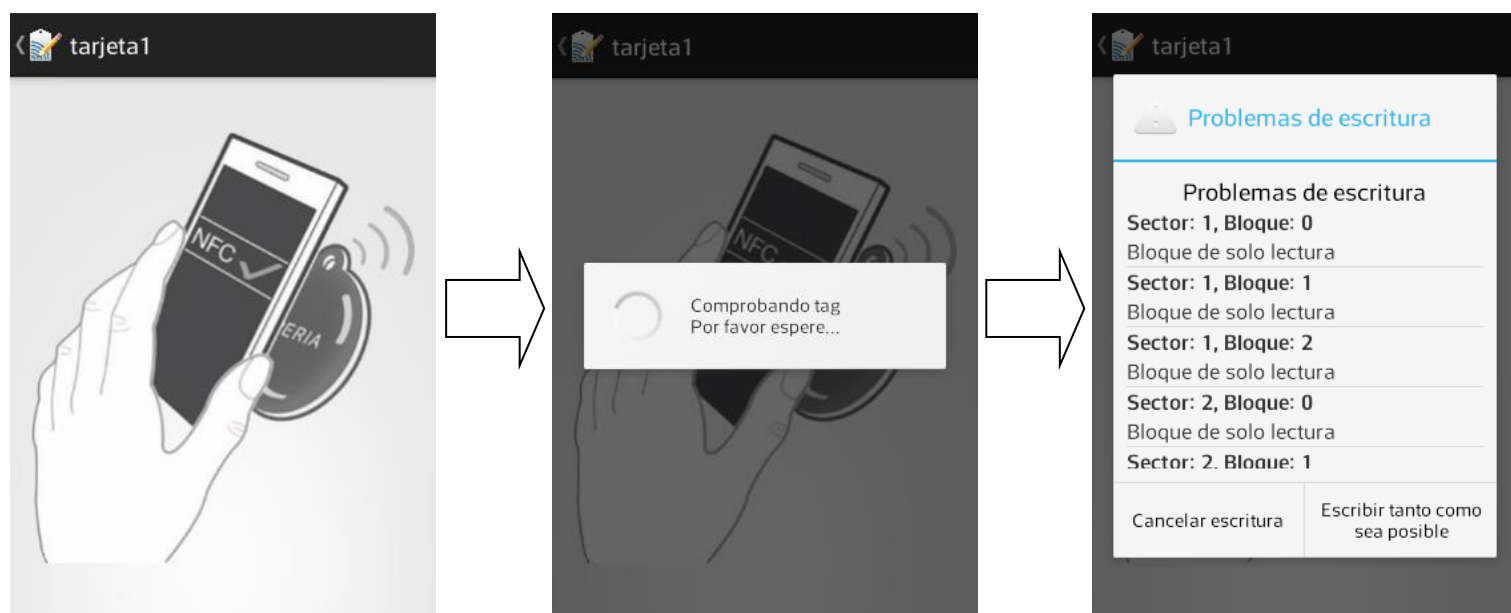


Ilustración 56: Manual de usuario – Escribir todos los bloques posibles

## 5. Ver tarjetas escaneadas

Esta funcionalidad consiste ver y gestionar todas las tarjetas que han sido almacenadas en el dispositivo móvil.

Para acceder a esta opción hay que pinchar sobre el icono Ver escaneados.



Ilustración 57: Manual de usuario – Acceder a escaneados

Aparecerá un listado con todas las tarjetas almacenadas en el teléfono, ordenadas alfabéticamente y clasificadas según el tipo de tarjeta. También aparecerá la categoría “Todos” donde se listan todas las tarjetas junto con el tipo al que pertenece.

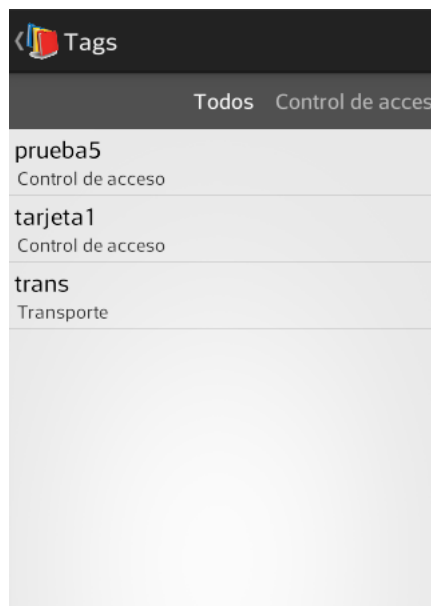


Ilustración 58: Manual de usuario – Lista de tarjetas

### 5.1. Crear tarjeta

Esta función permite crear el contenido de una tarjeta nueva con todo su contenido vacío. Para ello hay que acceder al listado de tarjetas almacenadas (ver apartado 5 Ver tarjetas escaneadas) y hacer click sobre la opción “Crear tag” del menú de opciones.

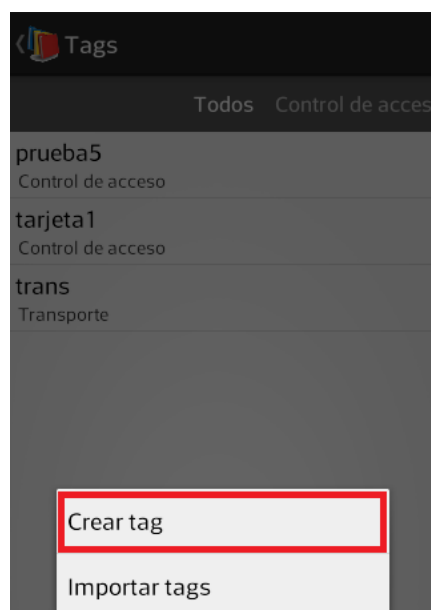
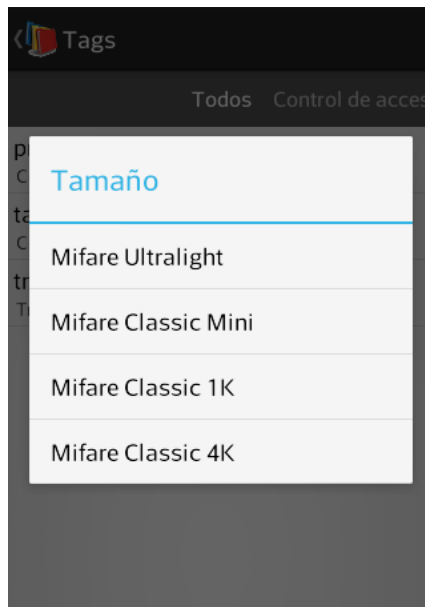


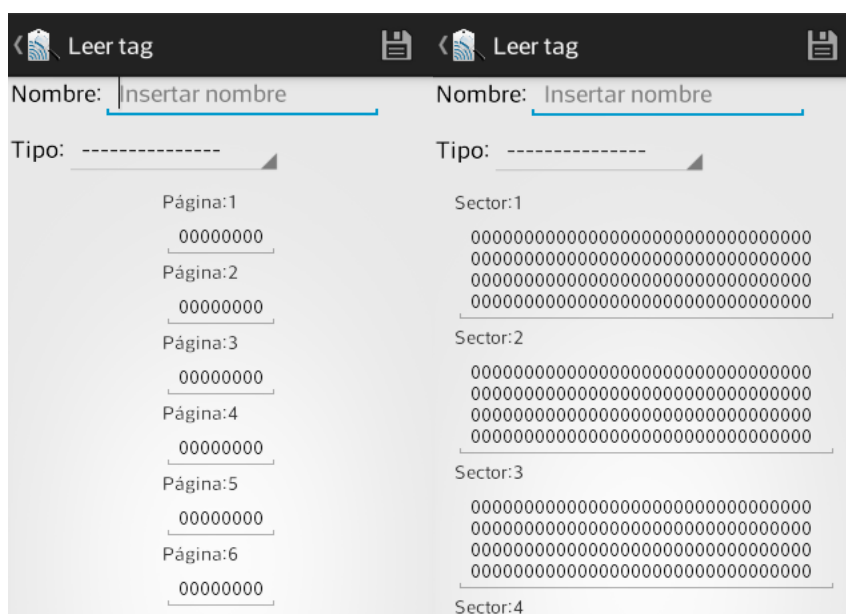
Ilustración 59: Manual de usuario – Crear tarjeta

A continuación hay que indicar el tipo de tarjeta que se desea crear: Mifare Ultralight, Mifare Classic Mini, Mifare Classic 1K o Mifare Classic 4K.



**Ilustración 60:** Manual de usuario – Seleccionar tipo de tarjeta a crear

Al pulsar sobre un tipo se rellenará todo su contenido con caracteres con valor 0. A continuación se muestra la apariencia de una tarjeta creada del tipo Mifare Ultralight (izquierda) y Mifare Classic (derecha).



**Ilustración 61:** Manual de usuario – Tarjeta Mifare Ultralight creada (izquierda); Tarjeta Mifare Classic Mini, 1K y 4K creada (derecha)

## 5.2. Editar tarjeta

Esta función permite modificar una tarjeta que ya haya sido almacenada en el dispositivo móvil. Para ello hay que acceder al listado de tarjetas almacenadas (ver apartado 5 Ver tarjetas escaneadas) y hacer click sobre la tarjeta a modificar.

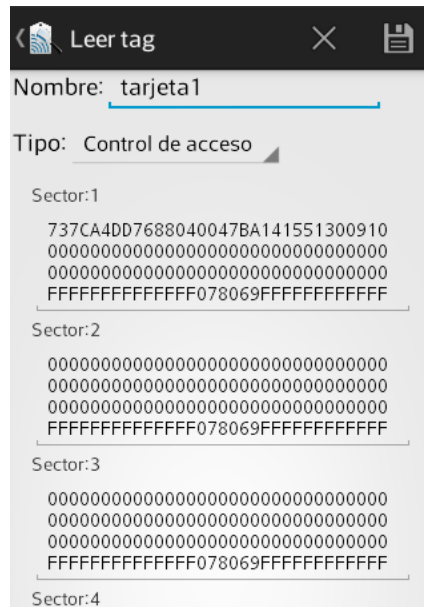


Ilustración 62: Manual de usuario – Editar tarjeta

Posteriormente se realizan las modificaciones deseadas (nombre, tipo o contenido de la tarjeta) y se pulsa sobre el botón Guardar del menú de opciones.

## 5.3. Borrar tarjeta

Esta función permite eliminar una tarjeta que ya haya sido almacenada previamente en el dispositivo móvil. Para ello hay que acceder al listado de tarjetas almacenadas (ver apartado 5) y mantener pulsada la tarjeta a eliminar.

Aparecerá un diálogo en el que hay que pulsar sobre el botón Aceptar para confirmar la acción.



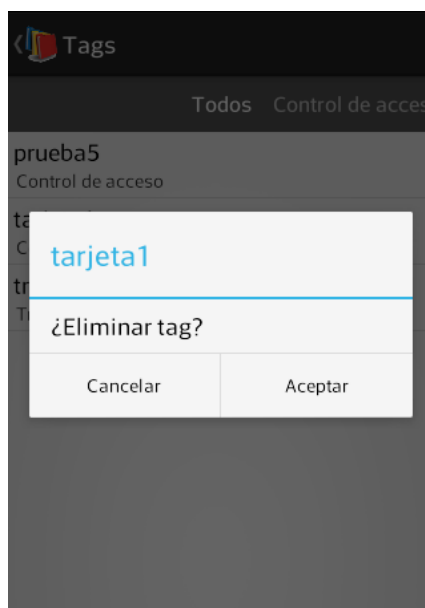


Ilustración 63: Manual de usuario – Eliminar tarjeta

Volverá a mostrarse el listado de tarjetas almacenadas pero sin la tarjeta eliminada.

#### 5.4. Importar tarjetas

Esta función permite importar el contenido de tarjetas desde ficheros ubicados en el dispositivo móvil. Para ello hay que acceder al listado de tarjetas almacenadas (ver apartado 5 Ver tarjetas escaneadas) y hacer click sobre la opción “Importar tags” del menú de opciones.



Ilustración 64: Manual de usuario – Importar tarjetas

A continuación aparecerá un diálogo donde se debe indicar la siguiente información y pulsar sobre el botón Aceptar:

- **Ruta:** ruta de la carpeta donde están almacenadas las tarjetas a importar. Si se indica el nombre de un fichero solo se importará esa tarjeta y si se indica la ruta de una carpeta se importarán todas las tarjetas que haya en ese directorio.
- **Importar claves:** si se marca esta opción las claves de la tarjeta serán almacenadas en el dispositivo móvil.

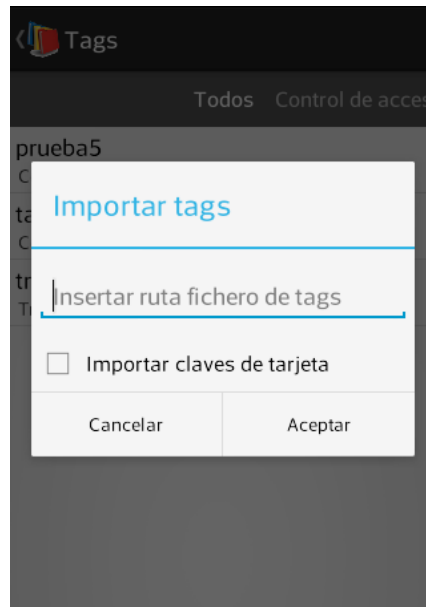


Ilustración 65: Manual de usuario – Importar tarjetas – Configuración

Si la importación termina correctamente aparecerá el mensaje “Tags almacenados”, sino el mensaje de error correspondiente.

**Nota:** el nombre de los ficheros a importar deben tener el formato *NOMBRE\_TIPO.dmp*, donde:

- **Nombre:** corresponde al nombre que se le asignará a la tarjeta cuando se almacene en el dispositivo.
- **Tipo:** corresponde al tipo de tarjeta. Puede ser *mfu* (Mifare Ultralight), *mfcmm* (Mifare Classic Mini), *mfc1k* (Mifare Classic 1K) y *mfc4k* (Mifare Classic 4K).

## 6. Claves

Esta funcionalidad consiste en la gestión de las claves almacenadas en el dispositivo móvil.

Para acceder a esta opción hay que pinchar sobre el icono Claves.

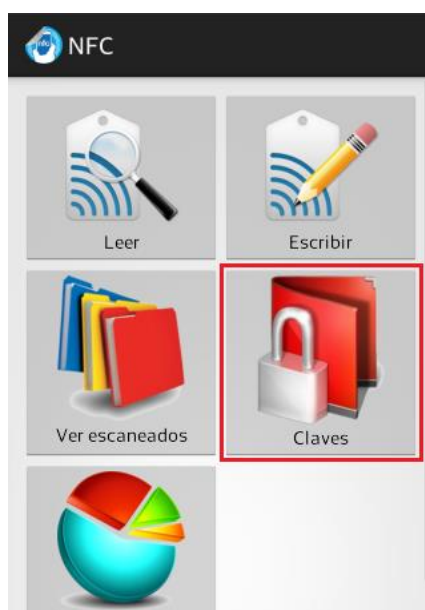


Ilustración 66: Manual de usuario – Acceder a claves

Aparecerá una pantalla con dos secciones:

- **Todos:** muestra las claves almacenadas en el dispositivo móvil. Existen dos tipos:
  - **Sistema:** claves por defecto del sistema y que no pueden ser modificadas ni eliminadas.
  - **Personalizada:** claves insertadas o importadas por el usuario. Estas claves pueden ser modificadas y eliminadas.
- **Grupos:** muestra todos los grupos de claves almacenados en el dispositivo móvil.

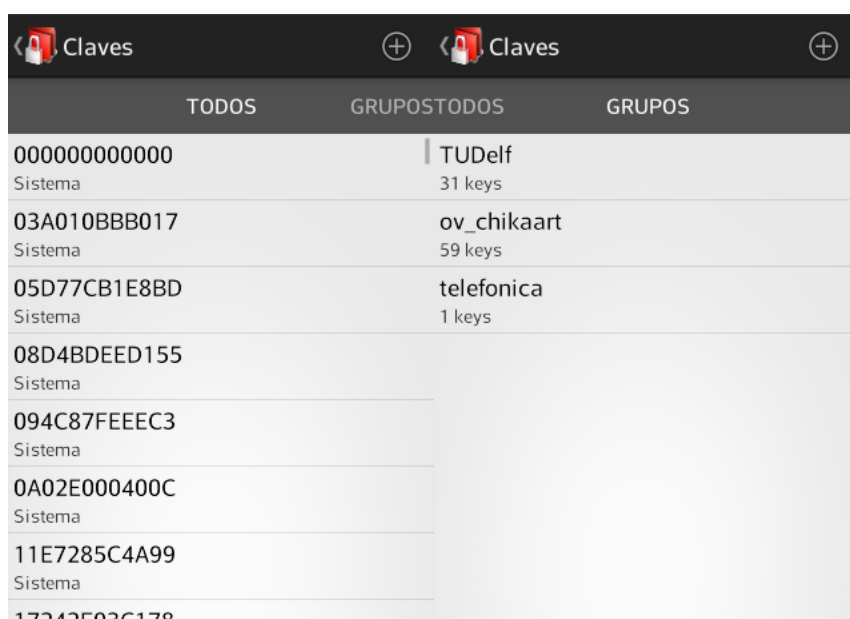


Ilustración 67: Manual de usuario – Lista de claves (izquierda) y grupos de claves (derecha)

## 6.1. Crear clave

Esta función permite crear una nueva clave. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves) y hacer click sobre la opción “Nuevas claves” del menú de opciones.

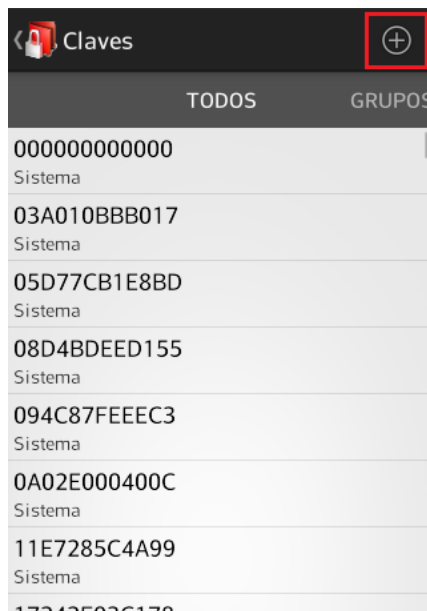


Ilustración 68: Manual de usuario – Crear clave

Aparecerá un diálogo solicitando que se introduzca la nueva clave. Para introducir varias claves al mismo tiempo cada una de ellas debe ir escrita en una línea diferente.

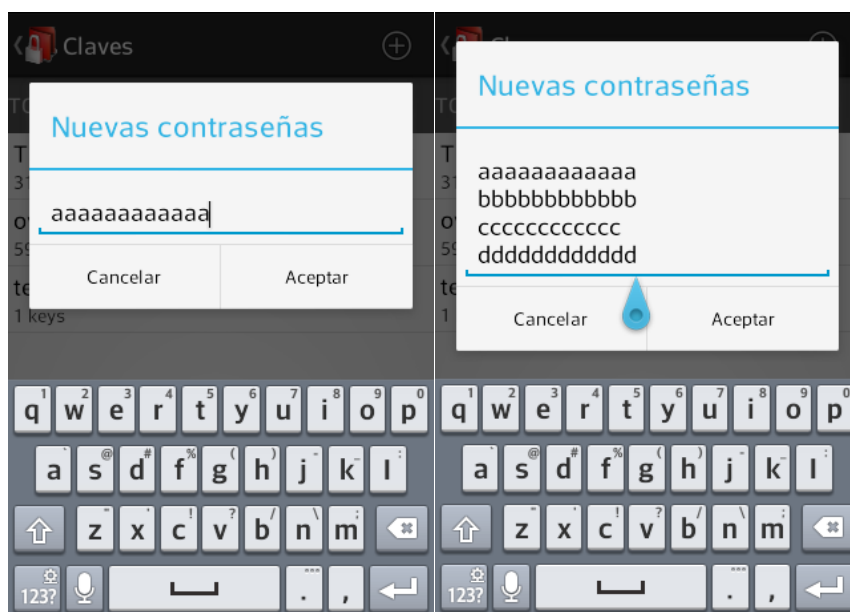


Ilustración 69: Manual de usuario – Crear una clave (izquierda); varias claves (derecha)

Por último hacer click en el botón Aceptar para confirmar la acción. Si las claves son almacenadas correctamente aparecerá el mensaje “Claves almacenadas”, sino el mensaje de error correspondiente.

**Nota:** las claves deben contener 12 caracteres hexadecimales (del 0 al 9 y ABCDEF).

## 6.2. Editar clave

Esta función permite modificar una clave ya almacenada. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves) y hacer click sobre la clave a editar.

Aparecerá un diálogo solicitando introducir la nueva clave.



Ilustración 70: Manual de usuario – Editar clave

Por último hacer click en el botón Aceptar para confirmar la acción. Si las claves son almacenadas correctamente aparecerá el mensaje “Clave modificada”, sino el mensaje de error correspondiente.

**Nota:** las claves deben contener 12 caracteres hexadecimales (del 0 al 9 y ABCDEF).

## 6.3. Borrar clave

Esta función permite eliminar una clave ya almacenada. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves) y mantener pulsada la clave a eliminar.

Aparecerá un diálogo en el que hay que pulsar sobre el botón Aceptar para confirmar la acción.

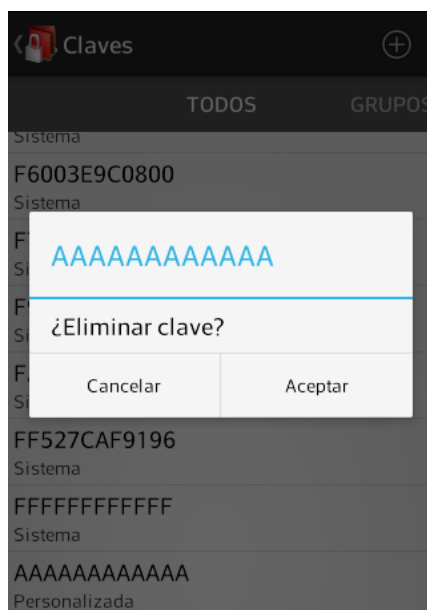


Ilustración 71: Manual de usuario – Eliminar clave

Volverá a mostrarse el listado de claves almacenadas pero sin la clave eliminada.

## 6.4.Importar claves

Esta función permite importar claves desde ficheros ubicados en el dispositivo móvil. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves) y hacer click sobre la opción “Importar claves” del menú de opciones.



Ilustración 72: Manual de usuario – Importar claves

A continuación aparecerá un diálogo donde se debe indicar la ruta donde se encuentran los ficheros de claves a importar.



**Ilustración 73:** Manual de usuario – Importar claves – Configuración

Si la importación termina correctamente aparecerá el mensaje “Claves almacenadas”, sino el mensaje de error correspondiente.

**Nota:** los ficheros deben tener extensión *.txt* y los claves que posea deben estar formadas por 12 caracteres hexadecimales (del 0 al 9 y ABCDEF).

## 6.5. Grupos de claves

Los grupos de claves son conjuntos de claves ya almacenadas en el teléfono.

### 2.3.1. Crear grupo de claves

Esta función permite crear un nuevo grupo de claves. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves) y hacer click sobre la opción “Crear grupo de claves” del menú de opciones.



Ilustración 74: Manual de usuario – Crear grupo de claves

Aparecerá un diálogo solicitando que se introduzca:

- **Nombre:** nombre del grupo de claves a crear. Este nombre es único por lo que no podrá existir otro grupo con este nombre.
- **Claves:** seleccionar las claves que van a componer este grupo de claves.

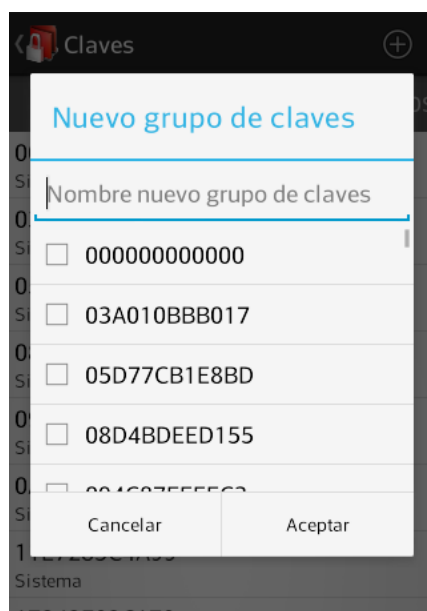


Ilustración 75: Manual de usuario – Crear grupo de claves

Por último hacer click en el botón Aceptar para confirmar la acción. Si el grupo de claves es almacenado correctamente aparecerá el mensaje “Grupo de claves almacenado”, sino el mensaje de error correspondiente.



**Nota:** las claves utilizadas para crear el grupo de claves deben haber sido almacenadas previamente.

### 2.3.2. Editar grupo de claves

Esta función permite modificar un grupo de claves ya almacenado. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves), acceder a la sección de grupos de claves y hacer click sobre el grupo de claves a modificar.

Aparece una nueva pantalla listando las claves que forman el grupo de claves.

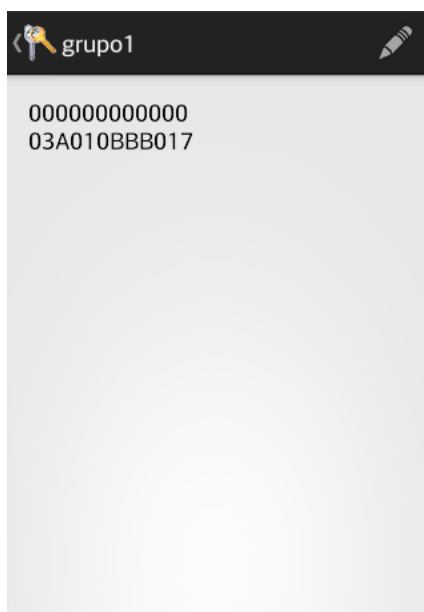


Ilustración 76: Manual de usuario – Claves de grupo de claves

A continuación hay que hacer click sobre la opción “Editar” del menú de opciones.

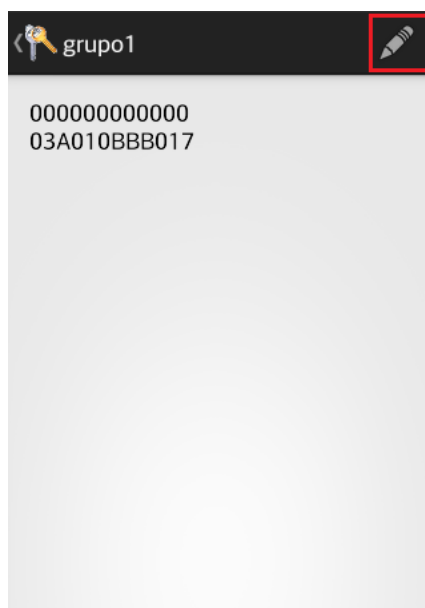


Ilustración 77: Manual de usuario – Editar grupo de claves – Opción menú

Posteriormente aparecerá un diálogo solicitando que se modifique la información deseada (nombre o claves del grupo de claves).



Ilustración 78: Manual de usuario – Editar grupo de claves

Por último hacer click en el botón Aceptar para confirmar la acción. Si el grupo de claves es almacenado correctamente aparecerá el mensaje “Grupo de claves modificado”, sino el mensaje de error correspondiente.

**Nota:** las claves utilizadas para editar el grupo de claves deben haber sido almacenadas previamente.

### 2.3.3. Borrar grupo de claves

Esta función permite eliminar un grupo de claves ya almacenado. Para ello hay que acceder al listado de claves almacenadas (ver apartado 6 Claves), acceder a la sección de grupos de claves y mantener pulsado el grupo de claves a eliminar.

Aparecerá un diálogo en el que hay que pulsar sobre el botón Aceptar para confirmar la acción.



Ilustración 79: Manual de usuario – Eliminar grupo de claves

Volverá a mostrarse el listado de grupos de claves almacenados pero sin el grupo eliminado.

## 7. Ver estadísticas de uso

Esta funcionalidad consiste en visualizar las estadísticas de uso de las claves utilizadas para las operaciones con las tarjetas RFID.

Para ver las estadísticas hay que pinchar sobre el icono de la operación estadísticas.



**Ilustración 80: Manual de usuario – Acceder a escribir**

Aparecerá un listado con todas las claves que se han utilizado en algún momento para la lectura o escritura de tarjetas RFID.

Este listado está compuesto por 4 campos:

- **Clave:** clave con la que se ha realizado la operación.
- **Nº Lecturas:** indica el número de veces que la clave ha sido utilizada para leer una tarjeta RFID.
- **Nº Escrituras:** indica el número de veces que la clave ha sido utilizada para escribir una tarjeta RFID.
- **Porcentaje:** indica el porcentaje del número total de veces que se ha utilizado la clave (lectura y escritura) con respecto a todos los usos de todas las claves. Las claves son ordenadas de mayor a menor según el valor de este campo.

Estadísticas de uso			
Clave	Nº Lecturas	Nº Escrituras	Porcentaje
FFFFFFFFFFFF	351	17	14,59
FF527CAF9196	27	0	1,07
FAC3A09DB433	27	0	1,07
F3F882A721D0	27	0	1,07
ED15A2390382	27	0	1,07
DCEC4B4FBECC	27	0	1,07
D8F06C7839F9	27	0	1,07
D4663050F031	27	0	1,07
C0192697C60D	27	0	1,07
RF08504FAA8B0	27	0	1,07

**Ilustración 81: Manual de usuario – Seleccionar tarjeta a escribir**

## 8. Activar tecnología NFC

Este es un mecanismo que cada vez que la aplicación es iniciada comprueba si el dispositivo posee tecnología NFC, y si es así comprueba si está activada. En caso de que no esté activada muestra un diálogo ofreciendo acceder a la sección “Conexiones inalámbricas” de los ajustes del dispositivo móvil y activarla.



Ilustración 82: Manual de usuario – Activar tecnología NFC

# ANEXO IV:

## Scripts y Modificaciones de Aplicaciones

---

Para el desarrollo de este proyecto se ha visto necesario crear una serie de scripts y modificar el código de otras aplicaciones. En este anexo se indican dichos elementos.

### **Scripts de instalación**

En este punto se especifican los scripts en lenguaje BASH utilizados para las reiterativas instalaciones del software LibNFC y Mfoc en PC y el dispositivo móvil, y Proxmark3 en el dispositivo móvil. En ambas máquinas la instalación se ha hecho sobre una máquina virtual Linux.

#### Script de instalación Proxmark3 en dispositivo móvil

```
#!/bin/bash

su

mount

mount -o remount /dev/block/platform/omap/omap_hsmmc.0/by-name/system /system

cd system

chmod 777 lib

chmod 777 bin

dd if=/sdcard/libusb.so of=/system/lib/libusb.so

dd if=/sdcard/libreadline.so of=/system/lib/libreadline.so

dd if=/sdcard/libtermcap.so of=/system/lib/libtermcap.so

dd if=/sdcard/proxmark3 of=/system/bin/proxmark3
```

#### Script de instalación LibNFC y Mfoc en PC y dispositivo móvil

```
#!/bin/bash

#-----

#LibNFC

#-----

sudo apt-get install build-essential subversion automake autoconf libusb-dev
libpcsc-lite-dev libusb-0.1-4 libpcsc-lite1 pcscd pcsc-tools libtool flex
libccid libacscid1

wget http://libnfc.googlecode.com/files/libnfc-1.7.0-rc7.tar.gz

tar -xvzf libnfc-1.7.0-rc7.tar.gz
```

---

```
rm libnfc-1.7.0-rc7.tar.gz

cd libnfc-1.7.0-rc7

autoreconf -vis

./configure --with-drivers=acr122_pcsc && make clean all

sudo make install

cd ..

sudo ldconfig

#-----

#Mfoc

#-----

wget https://mfoc.googlecode.com/files/mfoc-0.10.6.tar.gz

tar xvf mfoc-0.10.6.tar.gz

cd mfoc-0.10.6/

autoreconf -vis

automake

autoconf

./configure

make all

sudo make install
```

### Modificación de LibNFC

Debido a que LibNFC posee escasa documentación se ha visto necesario realizar una serie de modificaciones en el código fuente para entender su funcionalidad.

Estas modificaciones han consistido en añadir mensajes de depuración para saber cuál es la situación de la aplicación en cada momento. Además estos mensajes han servido para conocer la información y los comandos enviados entre el lector y la tarjeta RFID, tanto en formato hexadecimal como ASCII.

Estas modificaciones se han hecho en lenguaje C.



**Modificación de Proxmark3 para el dispositivo móvil**

Esta aplicación solo se ha modificado para que las claves obtenidas sean legibles para el usuario ya que inicialmente eran codificadas en base octal.

Estas modificaciones se han hecho en lenguaje C.

**Modificación de programa Mfoc GUI**

Este programa se ha modificado únicamente para obtener la base de datos utilizada para decorar la información de una tarjeta de transporte y así poder utilizarla desde el dispositivo móvil.

Estas modificaciones se han hecho en lenguaje C#.

